

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 1 月 2 1 日
Date of Application:

出 願 番 号 特 願 2 0 0 4 - 0 1 2 9 0 4
Application Number:
[ST. 10/C] : [J P 2 0 0 4 - 0 1 2 9 0 4]

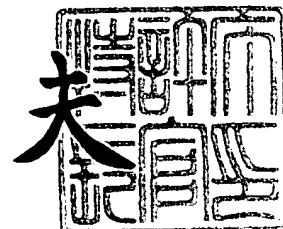
出 願 人 株式会社リコー
Applicant(s):

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 4 年 2 月 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0400503
【提出日】 平成16年 1月21日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G03G 21/00 370
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 毛呂井 昭平
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2003- 19721
 【出願日】 平成15年 1月29日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置であって、

認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、

当該認証モジュールは、前記システム側ソフトウェアとは別に備えられていることを特徴とする画像形成装置。

【請求項 2】

前記システム側ソフトウェアは認証機能部を含み、

利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行う請求項 1 に記載の画像形成装置。

【請求項 3】

前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行する手段、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する手段を有する請求項 1 又は 2 に記載の画像形成装置。

【請求項 4】

前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する認証モジュール実行手段を有する請求項 1 又は 2 に記載の画像形成装置。

【請求項 5】

前記認証モジュールは、J a v a（登録商標）プログラムであり、前記認証モジュール実行手段は、クラスライブラリと仮想マシンを含む請求項 4 に記載の画像形成装置。

【請求項 6】

前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、

前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う請求項 1 又は 2 に記載の画像形成装置。

【請求項 7】

前記画像形成装置は、前記携帯端末から前記認証用データを入力させるための画面データを生成し、当該画面データを前記携帯端末に送信する手段を有する請求項 6 に記載の画像形成装置。

【請求項 8】

前記認証用データとして、部署名又はアプリケーションの使用目的を利用者に入力させる請求項 1 ないし 7 のうちいずれか 1 項に記載の画像形成装置。

【請求項 9】

前記認証モジュールの認証用画面を、前記画像形成装置の立ち上がり時に優先的に前記オペレーションパネルに表示させる手段を有する請求項 1 又は 2 に記載の画像形成装置。

【請求項 1 0】

前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力となされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる手段を有する請求項 1 又は 2 に記載の画像形成装置。

【請求項 1 1】

前記画像形成装置は、所定のジョブが終了した後、一定時間の経過を検出した場合に前

記システムオートクリアを起動し、前記認証用画面を表示する請求項 10 に記載の画像形成装置。

【請求項 12】

前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する手段を有する請求項 1 又は 2 に記載の画像形成装置。

【請求項 13】

前記認証モジュールは、前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告表示をさせる請求項 12 に記載の画像形成装置。

【請求項 14】

アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置における認証方法であって、

前記画像形成装置に前記システム側ソフトウェアとは別に認証モジュールを備え、該認証モジュールが、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させることを特徴とする認証方法。

【請求項 15】

前記システム側ソフトウェアは認証機能部を含み、

利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行う請求項 14 に記載の認証方法。

【請求項 16】

前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する請求項 14 又は 15 に記載の認証方法。

【請求項 17】

前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する請求項 14 又は 15 に記載の認証方法。

【請求項 18】

前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、

前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う請求項 14 又は 15 に記載の認証方法。

【請求項 19】

前記画像形成装置は、前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力となされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる請求項 14 又は 15 に記載の認証方法。

【請求項 20】

前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する請求項 14 又は 15 に記載の認証方法。

【請求項 21】

アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置に、

認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証手順を実

行させるプログラムであって、前記システム側ソフトウェアとは別に前記画像形成装置に備えられることを特徴とするプログラム。

【請求項 2 2】

前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、

前記プログラムは、前記通信手段により前記携帯端末から受信した認証用データを用いて前記認証手順を前記画像形成装置に実行させる請求項 2 1 に記載のプログラム。

【請求項 2 3】

前記画像形成装置の利用に関するログ情報を収集する手順を前記画像形成装置に実行させる請求項 2 1 に記載のプログラム。

【請求項 2 4】

前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告を表示させる手順を前記画像形成装置に実行させる請求項 2 3 に記載のプログラム。

【請求項 2 5】

請求項 2 1 ないし 2 4 のうちいずれか 1 項に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】明細書

【発明の名称】画像形成装置、認証方法、及びプログラム

【技術分野】

【0001】

本発明は画像形成装置に係り、特に、認証機能を備えた画像形成装置に関する。

【背景技術】

【0002】

従来から、プリンタやコピー機等の画像形成装置に利用者制限モードを設け、使用時にユーザーコードを入れて認証することで、利用制限を解除する方式がある。また、プリンタ、コピー、ファクシミリ、スキャナなどの各装置の機能を1つの筐体内に収納した画像形成装置にも利用者制限モードが設けられている。

【0003】

また、上記の画像形成装置にキーカード、プリペイドカード、コインラックやカードリーダーなどの装置を接続し、カードのセットやコインの投入により、利用制限解除や課金管理を可能とする方式も普及している。

【特許文献1】特開2002-149362号公報

【特許文献2】特開2002-108583号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

上記の利用制限等の目的は、画像形成装置が使用される組織や企業等のユーザーにより様々であり、各ユーザーの目的に応じた方法で利用制限や課金管理を行う手段を実装した画像形成装置を迅速に提供することが要望されている。

しかしながら、従来の技術における利用制限のための認証は、画像形成装置に固定的に備えられるシステムソフトウェアに認証機能を含めることによって実現していたので、各ユーザーの希望に応じて認証機能をカスタマイズすることを迅速に行うことはできなかった。

【0005】

更に、利用制限や課金管理の目的によっては、その方法を変更しなければならない場合があり、利用制限や課金管理の方法を容易に変更できることが要望されている。しかし、従来のようにシステムソフトウェアに利用制限のための認証機能を組み込む方式では、システムにおける一部の機能のみを変更することは、変更をする予定のない他の機能に与える影響も大きいことから、容易ではなかった。

【0006】

本発明は、上記の点に鑑みてなされたものであり、種々の目的に応じた認証機能を容易に追加、変更することを可能とする画像形成装置、認証方法及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【0007】

上記の目的は、以下の発明の構成により達成できる。

【0008】

請求項1に記載の発明は、アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置であって、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、当該認証モジュールは、前記システム側ソフトウェアとは別に備えられていることを特徴とする画像形成装置である。

【0009】

本発明によれば、認証条件を満たさない限り認証用画面から画像形成装置の使用画面に

移行させないようにでき、利用制限をかけることができる。これにより、認証用画面及び認証条件を適宜設定すれば、種々の目的に応じた利用制限が可能となる。また、ROM等に固定的に備えられるシステム側ソフトウェアとは別に認証モジュールを設けたため、認証モジュールを容易に追加、変更することが可能となる。

【0010】

請求項2に記載の発明は、請求項1に記載の画像形成装置において、前記システム側ソフトウェアは認証機能部を含み、利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行うものである。

【0011】

本発明によれば、システム側ソフトウェアの認証機能と、追加的に搭載される認証モジュールとを、アプリケーション毎に選択的に使用することが可能となる。

【0012】

請求項3に記載の発明は、請求項1又は2に記載の画像形成装置において、前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行する手段、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する手段を有するものである。

【0013】

本発明によれば、カスタマイズした認証モジュールを必要に応じて実行させることが可能となる。

【0014】

請求項4に記載の発明は、請求項1又は2に記載の画像形成装置において、前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する認証モジュール実行手段を有する。また、請求項5に記載の発明は、請求項4に記載の画像形成装置において、前記認証モジュールは、Java（登録商標）プログラムであり、前記認証モジュール実行手段は、クラスライブラリと仮想マシンを含む。このような構成によれば、認証モジュールの追加変更を一層容易に行うことが可能となる。

【0015】

請求項6に記載の発明は、請求項1又は2に記載の画像形成装置において、前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う。また、請求項7に記載の発明は、請求項6に記載の画像形成装置において、前記画像形成装置は、前記携帯端末から前記認証用データを入力させるための画面データを生成し、当該画面データを前記携帯端末に送信する手段を有するというものである。

【0016】

本発明によれば、オペレーションパネルのみならず、PDA、携帯電話等の携帯端末から認証用データを入力することができる。

【0017】

請求項8に記載の発明は、請求項1ないし7のうちいずれか1項に記載の画像形成装置において、前記認証用データとして、部署名又はアプリケーションの使用目的を利用者に入力させるものである。これにより、種々の目的に応じた認証を行うことが可能となる。

【0018】

請求項9に記載の発明は、請求項1又は2に記載の画像形成装置において、前記認証モジュールの認証用画面を、前記画像形成装置の立ち上がり時に優先的に前記オペレーションパネルに表示させる手段を有するものである。本発明によれば、電源を投入してすぐに認証画面を表示させ、利用制限を行うことが可能となる。

【0019】

請求項 10 に記載の発明は、請求項 1 又は 2 に記載の画像形成装置において、前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力となされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる手段を有するものである。

【0020】

本発明によれば、画像形成装置の使用中にその場から離れた後にジョブが終了しても、自動的に認証用画面を表示させることができる。また、画像形成装置を放置していた場合等に、システムオートクリア機能が作動した場合にも、認証用画面を表示させることができる。また、画像形成装置の使用中に認証モジュールを使用するためのキー入力をしておけば、認証用画面を表示させることができる。これらにより、他人による不正使用を防止することが可能となる。

【0021】

請求項 11 に記載の発明は、請求項 10 に記載の画像形成装置において、前記画像形成装置は、所定のジョブが終了した後、一定時間の経過を検出した場合に前記システムオートクリアを起動し、前記認証用画面を表示するというものである。

【0022】

請求項 12 に記載の発明は、請求項 1 又は 2 に記載の画像形成装置において、前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する手段を有するというものである。

【0023】

また、請求項 13 に記載の発明は、請求項 12 に記載の画像形成装置において、前記認証モジュールは、前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告表示をさせるものである。

【0024】

請求項 14 ～請求項 19 に記載の発明は、上記画像形成装置における認証方法の発明である。請求項 20 ～請求項 24 に記載の発明は、上記画像形成装置の認証モジュールに対応するプログラムである。請求項 25 に記載の発明は、上記プログラムを記録した記録媒体の発明である。

【発明の効果】

【0025】

本発明によれば、ROM 等に固定的に備えられるシステム側ソフトウェアとは別に認証モジュールを設けたため、容易に追加、変更可能な認証機能を備えた画像形成装置を提供できる。

【発明を実施するための最良の形態】

【0026】

(第 1 の実施の形態)

まず、本発明の第 1 の実施の形態の概要について、図 1、2 を用いて説明する。

【0027】

本実施の形態における画像形成装置（以下、複合機という）は、表示部、印刷部及び撮像部などの画像形成処理で使用するハードウェア資源を備えるとともに、プリンタ、コピー又はファクシミリなどのアプリケーションを複数搭載している。また、これらのアプリケーションとハードウェア資源との間に介在してハードウェア資源の管理、実行制御並びに画像形成処理を行う各種コントロールサービスを備えている。この複合機は、アプリケーションを追加することが従来の複合機に比べて容易にできるので、ユーザーのニーズに応じたアプリケーションを開発し、既にユーザーサイドで稼動している複合機に必要な応じて新規アプリケーションを追加することが可能である。なお、コントロールサービスはシステム側ソフトウェアと称することができる。

【0028】

この複合機では、各アプリケーションに対して、図1に示すような共通の操作部（以下、オペレーションパネルという）を使用する。アプリケーション切り替えは、オペレーションパネルにおけるアプリケーション切り替えキーを押下しすることで行うことができる。

本実施の形態における複合機は、本発明に係る認証モジュールを備える。認証モジュールは、システム側に固定的に備えられている認証機能とは別に設けられているものである。この認証モジュールによる画面がオペレーションパネルに表示されている場合、認証条件をクリアしない限り、画面を他のアプリケーション等に切り替えることができない。なお、認証モジュールが使用する認証のための情報は複合機内に備えていてもよいし、認証情報を外部の認証・課金サーバに置き、当該認証・課金サーバにネットワークを介して認証を依頼するような構成としてもよい。

【0029】

また、本実施の形態における複合機では、認証モジュールを“優先アプリ”に設定することができる。優先アプリとは、電源ON時又はシステムリセット時に画面の制御権を持って立ち上がるアプリケーションである。優先アプリは、複合機が立ち上がった際にオペレーションパネルの画面制御権を持っている。従って、認証モジュールを“優先アプリ”に設定することで、認証条件をクリアしない限り、所望のアプリケーションの利用が制限される。なお、“優先アプリ”として設定できるものは、いわゆるアプリケーションに限られず、システム側のソフトウェアでもよい。すなわち、本明細書における“優先アプリ”は、アプリケーション及びシステム側のソフトウェアを含む意味で使用する。

【0030】

認証・課金サーバを用いる場合の全体の構成例を図2に示す。図2は、複合機100と認証・課金サーバ150とがネットワークを介して接続される構成を示している。

【0031】

図2に示す構成における複合機の動作の概要を次に説明する。

【0032】

認証モジュールが優先アプリとして立ち上がると、オペレーションパネルの画面には認証を行うため「ユーザーコード」及び「パスワード」の入力画面を表示する。また、複合機に備えられたカードリーダーを用いてカードから情報を取得する場合には、「カードを通してください」等の表示を行う。

【0033】

ユーザーコードを用いる例について説明すると、まず複合機100を使用したいユーザーは、ユーザーコードをオペレーションパネルの画面から入力する。複合機100はユーザーコードの入力を受け、ネットワーク上に有る認証・課金サーバ150に問い合わせを行う。認証・課金サーバ150側では、入力されたユーザーコードに一致するデータがあれば、認証OKの通知を認証モジュールに返答する。認証モジュールは、オペレーションパネルに、「利用したいアプリのキーを選択下さい」等と表示し、アプリ切り替えキーを有効にする。

【0034】

ここでユーザーがコピーキーを押下しすると、コピーの画面が表示され、原稿をセットしてコピーを開始できる。コピーが完了し、一定時間（タイマー設定：例えばアイドル状態30秒）経過し、システムオートクリアが起動されると、認証モジュールの画面を表示して利用制限モードに戻る。

【0035】

次に、本発明の第1の実施の形態をより詳細に説明する。

【0036】

図3は、本実施の形態における複合機の構成を示すブロック図である。図3に示すように、複合機100は、白黒ラインプリンタ（B&W LP）101と、カラーラインプリンタ（Color LP）102と、スキャナ、ファクシミリなどのハードウェアリソース103などを有するとともに、プラットフォーム120とアプリケーション130とから構成されるソフト

トウェア群 110 と、電源投入時に実行される複合機起動部 140 とを備えている。

【0037】

複合機起動部 140 は、複合機 100 の電源投入時にまずはじめに実行され、機器の初期化、診断を行い、各コントロールサービス、各アプリケーション等を起動するものである。

プラットフォーム 120 は、アプリケーション 130 からの処理要求を解釈してハードウェア資源の獲得要求を発生させるコントロールサービスと、一又は複数のハードウェア資源の管理を行い、コントロールサービスからの獲得要求を調停するシステムリソースマネージャ (SRM) 123 と、汎用 OS 121 とを有する。

【0038】

コントロールサービスは、複数のサービスモジュールから形成され、SCS (システムコントロールサービス) 122 と、ECS (エンジンコントロールサービス) 124 と、MCS (メモリコントロールサービス) 125 と、OCS (オペレーションパネルコントロールサービス) 126 と、FCS (ファックスコントロールサービス) 127 と、NCS (ネットワークコントロールサービス) 128 とから構成される。なお、このプラットフォーム 120 は、あらかじめ定義された関数により前記アプリケーション 130 から処理要求を受信可能とするアプリケーションプログラムインタフェース (API) を有する。

【0039】

汎用 OS 121 は、UNIX (登録商標) などの汎用オペレーティングシステムである。SRM 123 のプロセスは、SCS 122 とともにシステムの制御及びリソースの管理を行うものである。SCS 122 のプロセスは、アプリ管理、操作部制御、システム画面表示、LED 表示、リソース管理、割り込みアプリ制御等を行い、ECS 124 のプロセスは、ハードウェアリソース 103 のエンジンの制御を行う。なお、SCS 122 は、上記の管理機能に加えて、ユーザー認証の機能を含むものである。例えば、ユーザーから入力されたユーザコードとパスワードが、予め登録してあるユーザコードとパスワードに一致したときに複合機の使用を許可するといった機能を有している。

【0040】

MCS 125 のプロセスは、画像メモリ、ハードディスク装置 (HDD) の利用に関する処理を行う。また、FCS 127 のプロセスは、ファクシミリ送受信のための処理等を行う。NCS 128 は、ネットワーク I/O を必要とするアプリケーションに対して共通に利用できるサービスを提供するためのプロセスである。すなわち、NCS 128 は、データ通信のためのプロトコル処理等を行う機能を含むものである。

【0041】

OCS 126 のプロセスは、オペレータ (ユーザー) と本体制御間の情報伝達手段となるオペレーションパネル (操作パネル) の制御を行う。OCS 126 は、オペレーションパネルからキー押下をキーイベントとして取得し、取得したキーに対応したキーイベント関数を SCS 122 に送信する OCS プロセスの部分と、アプリケーション 130 又はコントロールサービスからの要求によりオペレーションパネルに各種画面を描画出力する描画関数やその他オペレーションパネルに対する制御を行う関数などがあらかじめ登録された OCS ライブラリの部分とから構成される。

【0042】

アプリケーション 130 は、プリンタ用のアプリケーションであるプリンタアプリ 111 と、コピー用アプリケーションであるコピーアプリ 112 と、ファクシミリ用アプリケーションであるファックスアプリ 113 と、スキャナ用アプリケーションであるスキャナアプリ 114 を有する。更に、必要に応じて複合機に追加される追加アプリ 115、116 を有している。これらの追加アプリは、フラッシュカード、SD カード等から必要に応じてインストール (ロード) できる。また、フラッシュカード、SD カード等から起動することも可能である。更に、ネットワークを介して他のサーバからインストール、及び起動することも可能である。

【0043】

更に、複合機 100 は、本発明に係る認証モジュール 117 を有している。認証モジュール 117 は、上記の追加アプリケーションと同様に、フラッシュカード、SD カード、ネットワーク接続されたサーバ等から容易に複合機に追加することが可能である。また、認証モジュールの機能変更をした場合には、容易に新しい認証モジュールをインストールすることが可能である。認証モジュールは、図 3 に示すように、コントロールサービス側に備えてもよいし、図 4 に示すようにアプリケーションとして備えてもよい。

【0044】

アプリケーション 130 の各プロセス、コントロールサービスの各プロセスは、関数呼び出しとその戻り値送信及びメッセージの送受信によってプロセス間通信を行いながら、その処理を実行している。そして、コントロールサービスがアプリケーション 130 に対し共通サービスを提供している。なお、コントロールサービスはシステム側ソフトウェアと称する場合がある。また、コントロールサービスによりアプリケーションに対して提供されるサービスをシステム側サービスと称する場合がある。

【0045】

図 5 は、図 3、4 に示した複合機 100 のハードウェア構成図である。図 5 に示すように、この複合機 100 は、コントローラボード 200 と、オペレーションパネル 210 と、ファックスコントロールユニット (FCU) 220 と、USB デバイス 230 と、IEEE 1394 デバイス 240 と、ブルートゥースデバイス 250 と、エンジン部 260 から構成されている。

【0046】

コントローラボード 200 は、ASIC 201、CPU 202、RAM 203、ROM 204、HDD 205、フラッシュカードインタフェース部 206、ネットワークインターフェースコントローラ 209 から構成されている。

【0047】

オペレーションパネル 210 は、ASIC 201 に直接接続されている。FCU 220、USB デバイス 230、IEEE 1394 デバイス 240、ブルートゥースデバイス 250 及びエンジン部 260 は、PCI バスを介して ASIC 201 に接続されている。

【0048】

ネットワークインターフェースコントローラ 209 は、ネットワーク 271 に接続されている他の機器と MAC アドレスなどを用いて通信する。FCU 220 は電話網 272 に接続されている。また、USB デバイス 230、IEEE 1394 デバイス 240 及びブルートゥースデバイス 250 により、他の端末 273～275 に接続することができる。他の端末 273～275 としては、PC の他、PDA、携帯電話等でもよい。フラッシュカードインタフェース部 206 は、挿入されたフラッシュカード 207 とデータのやりとりを行うインタフェースである。更に、SD カードインタフェース部を備えてもよい。

【0049】

ROM 204 には、上述の各アプリケーション、プラットフォーム 120 を構成する各コントロールサービス及び SRM 123 の各プログラムが格納されている。

【0050】

本実施の形態では、認証モジュール 117 は、フラッシュカード 207 から直接起動するが、フラッシュカード 207 から HDD 205 にインストールして起動してもよい。プリンタアプリ 111、コピーアプリ 112、ファックスアプリ 113、スキャナアプリ 114 などのアプリケーション 130、各コントロールサービスは出荷時に ROM 204 に組み込まれている。これらのアプリケーションやコントロールサービスは、複合機 100 の起動時（電源投入時）に複合機起動部 140 によって起動される。すなわち、SCS 122 が有する認証機能部は、出荷時に ROM 204 に組み込まれているので、その機能変更は容易でない。一方、認証モジュール 117 は、必要に応じてフラッシュカード、SD カード等から起動できるので、追加、変更が容易である。

【0051】

以下、本実施の形態における複合機 100 の動作について詳細に説明する。

【0052】

図6は、複合機100の立ち上げ時の動作を示すフローチャートである。なお、この処理は、複合機起動部140により実行される処理である。

【0053】

まず、電源投入もしくはリセット後、初期化処理が行われる（ステップS1）。初期化処理は、BIOS（Basic Input/Output System）及びブートローダ（Boot Loader）の起動、カーネル（Kernel）の起動、ハードウェアの初期化、診断等である。

【0054】

次に、ROM等のメモリ媒体におけるROMファイル（romfs形式のファイル）をサーチし（ステップS2）、メモリ媒体の所定位置に配置されたアプリ設定ファイルをサーチする（ステップS3）。例えば、図7に示すように、ROMとフラッシュカードにROMファイル（ROM0とROM1）があり、それぞれの先頭部分にアプリ設定ファイルが存在する。ROMの中のアプリ設定ファイルの例を図8（a）に示し、フラッシュカードの中のアプリ設定ファイルの例を図8（b）に示す。なお、図8中、“-2”等は起動優先度を示している。

【0055】

次に、ROMの中のアプリ設定ファイルを参照して、mount命令に従ってROMファイルシステム（romfs）をマウントし、マウント先のアプリ設定ファイル（図8（b））も参照して、アプリケーションの起動条件、順序をチェックし（ステップS4）、各種アプリケーション、SCSを含むコントロールサービスを起動する（ステップS5）。図7、8の例では、A→C→B→D→Eの順にアプリケーションが起動される。

【0056】

ハードディスク（HDD205）にもアプリケーションが置かれている場合には、ハードディスクのプログラムを起動するためのランチャーを起動する。ランチャーは、ハードディスクを起動後、ハードディスクの準備が完了するまで待ち（ステップS6）、その後、ROMファイル及びアプリ設定ファイルのサーチを行い、アプリ設定ファイルに従って、アプリケーションの起動を行う（ステップS7～S9）。

【0057】

図9は、コントロールサービスの1つであるSCS122の起動後の複合機100の動作を示すフローチャートである。

【0058】

アプリ設定ファイルに従ってSCSプロセスが起動すると、まず、オペレーションパネル210にウィンドウが表示され（ステップS11）、「お待ちください」等のメッセージが表示される。その間、起動した各アプリケーション（コピー、プリンタ等）のアプリ登録が行われる（ステップS12）。SCS122では、各アプリケーションからのアプリ登録依頼メッセージを受信して、RAM等にアプリケーションの識別ID等を格納することによりアプリ登録を行う。

【0059】

続いて、RAM203等の記憶装置の所定の領域（以下、これを優先アプリ領域という）を参照することにより優先アプリの設定があるか否かをチェックする（ステップS13）。記憶装置の優先アプリ領域に優先アプリの設定がなければ、デフォルトのアプリケーション（通常はコピーアプリ）が優先アプリとして設定され（ステップS14）、認証モジュールが優先アプリとして設定されていれば認証モジュールが優先アプリとなる（ステップS15）。

【0060】

あるアプリケーションを優先アプリ領域に優先アプリとして設定することは、そのアプリケーションに、オペレーションパネルへのアクセス権限を付与することを意味する。すなわち、画面制御権限を付与することを意味する。以下、認証モジュール117が優先アプリとして設定されている場合について説明する。認証モジュール117が優先アプリとして設定されると、SCS122は、認証モジュール117に対して画面制御権限付与の

通知メッセージを送信する（ステップS16）。

【0061】

認証モジュール117は、SCS122から画面制御権限付与のメッセージを受信すると、オペレーションパネル210に対してユーザー認証用の画面を表示する（ステップS17）。より詳細には、オペレーションパネル210に対する画面表示は、認証モジュール117の表示依頼によりOCS126が行う。すなわち、認証モジュール117がOCS126に対して表示すべき描画情報を指定して描画関数の呼び出しを行うことにより、OCS126が指定された描画情報の表示処理を行う。

【0062】

ユーザー認証用の画面に対するユーザーからの入力が入力が認証条件を満たせば（ステップS18のY）、機器利用許可のメッセージとともに、アプリケーションを選択してくださいとのメッセージがオペレーションパネルに表示される（ステップS19）。なお、オペレーションパネル210からのキー入力、ボタン押下などの操作は、OCS126とSCS122を介して認証モジュールに通知されるものである。

【0063】

ユーザーがオペレーションパネル210からアプリケーションを選択すると、選択されたアプリケーションはSCS122に通知され、SCS122は、優先アプリの設定内容を選択されたアプリケーションに変更する。そして、その選択されたアプリケーションに対して画面制御権限付与のメッセージを通知する。その後、選択されたアプリケーションの実行、処理が行われる（ステップS20）。

【0064】

アプリケーションの実行中においては、システムオートクリア、認証モジュールキー押下し、アプリケーションのジョブ終了のときなどに、認証モジュールに画面の制御権限が移行し、認証モジュールは認証画面を表示する。

【0065】

上記の例では、最初に優先アプリとして認証モジュール117が設定されているが、その設定は次のようにして行う。複合機100の初期設定画面から優先アプリ設定を選択し、図10に示すような、追加アプリ（認証モジュール等）を含む優先アプリ設定画面を表示させる。そして、その画面から所望の追加アプリを選択する。これにより、選択された追加アプリ名が優先アプリ領域に登録される。複合機起動時には、この情報をSCS122が参照することにより、優先アプリ設定の有無を判断し、複合機100の立ち上がり時に、認証モジュールに認証画面を表示させることが可能となる。

【0066】

図11は、認証モジュール117を用いた場合における、オペレーションパネル210の画面状態遷移図である。なお、図11は、コピーアプリに着目した図である。

【0067】

同図に示すように、電源ON又はリスタートにより、まず認証モジュール画面に遷移し、認証条件入力待ちになる（状態1）。ユーザーからの入力が入力が認証条件を満たさなければ、認証モジュール画面のままである。ユーザーからの入力が入力が認証条件を満たす場合（認証OKの場合）には、アプリ選択画面を表示してアプリ切替キーイベント待ちになり（状態2）、選択するアプリケーションの入力を受けて、当該アプリケーションの画面に移行する。

【0068】

例えば、コピーアプリを選択した場合、コピー用の画面が表示され、コピー可能になる（状態3）。そして、コピーアプリ動作中において、ジョブ終了、システムオートクリア、認証モジュールに遷移するためのキーイベント等により認証モジュール画面に戻る。

【0069】

次に、図12のフローチャートを参照して認証モジュール117の動作を説明する。図12の左側には、各動作に対応したオペレーションパネル210の表示内容を示している。オペレーションパネルへの表示及びオペレーションパネルからのデータ入力はOCS1

26を介して行われるが、図12ではSCS122、認証モジュール117、コピーアプリ112に着目し、OCS126を図示していない。

【0070】

同図中、最初は認証モジュール画面が表示されており、認証条件入力待ちの状態となっている（認証条件入力待ち期間P1）。この状態では、仮にアプリ切替キーイベントがSCS122に通知され、SCS122から認証モジュール117に対して画面解放要求が出されても、認証モジュール117はそれを受け付けず、SCS122に対してNGを返す。すなわち、認証条件入力待ち期間P1では、認証モジュール117は、認証条件を満たす入力がない限り画面解放要求に対してNGを返し、画面解放を許可しない。

【0071】

オペレーションパネル210からユーザーコードやパスワード等の認証情報が入力されると、SCS122はその認証情報を認証モジュール117に通知し、認証情報が正かどうかのチェックを行い、認証OKであれば、その旨をSCS122に通知する（認証チェック）。

【0072】

認証済み期間P2において、認証モジュール117はアプリ切替画面表示を行う。なお、アプリ切替画面表示はSCS122が行ってもよい。そして、アプリ切替画面表示中に、コピーアプリ112が選択されると、コピーアプリ切替キーイベントがSCS122に通知され、SCS122から画面解放要求が認証モジュール117に送られる。認証済みであるので、認証モジュール117は、画面解放OKをSCS122に対して通知する。

【0073】

そして、SCS122は優先アプリ領域にコピーアプリを設定し、画面制御権限付与の通知メッセージをコピーアプリに通知する。そして、コピーアプリ112は、コピー画面を表示する。

【0074】

その後、コピー使用期間P3において、コピーアプリが使用される。ここで、コピー中にオペレーションパネル210から所定のキーを押すなどして認証モジュール117が選択されると、認証モジュールキーイベントがSCS122に通知される。そして、SCS122はコピーアプリに対して画面解放要求を出すと、コピーアプリはSCS122に画面解放OKを通知する。そして、SCS122は、優先アプリ領域の設定を認証モジュール117にし、画面制御権限付与のメッセージを認証モジュール117に対して通知する。そして、認証モジュール117は認証モジュール画面を表示し、認証条件入力待ちとなる（認証条件入力待ち期間P4）。なお、コピー中に認証モジュール画面を表示させることを可能としたことにより、コピー中にその場を離れた場合でも、他人に無断でコピーをとられてしまうといったことを防止できる。

【0075】

コピー中に認証モジュールキーイベントを発生させない場合に、コピー終了後複合機100をしばらく放置しておくと、SCS122によりシステムオートクリアが作動し、SCS122が認証モジュール117に制御権限を移行させ、認証モジュール117は認証モジュール画面を表示し、認証条件入力待ち期間P5に入る。

【0076】

なお、コピー完了後に、認証モジュール117による利用制限の代わりに、SCS122による利用制限機能を動作させ、「カードを通して下さい」といった警告用のポップアップウィンドウを開いて利用を制限してもよい。

【0077】

上記のように、第1の実施の形態によれば、認証モジュール117により複合機100全体の利用制限をかけることができる。上記の例では、認証条件をユーザーコード等の合致としたが、その他、用途、要求に応じた認証条件を用い、その認証条件にあった認証画面を表示することが可能である。例えば、企業独自の社員カード、指紋等による認証を行うことができる。認証方法自体も特に限定されることはなく、例えば、複合機100自身

が認証条件をチェックする方法や遠隔の認証・課金サーバが認証条件をチェックする方法の何れの方法もとることができる。また、認証条件や認証方法を変更する場合には、認証モジュールを変更すればよく、他のアプリケーション（コピー、プリンタ、FAX等）やシステム側ソフトウェアを変更する必要がないため、容易にカスタマイズができる。

【0078】

また、コピー中に認証モジュール画面に画面遷移することができるので、大量のコピーをセットしてその場を立ち去っても、再び認証を行わない限り、他のアプリケーション画面へ移れない。従って、他人に不正に使用されてしまう恐れがなくなる。また、認証用のアプリケーション画面に移行させることを忘れて、複合機100の前から離れても、コピー完了後にシステムオートクリアが働いて認証画面を表示させることが可能なので、他人に不正に使用されてしまう恐れがなくなる。

【0079】

（第2の実施の形態）

次に、本発明の第2の実施の形態について説明する。第2の実施の形態は、コピーの枚数管理を行う場合において認証モジュール117が残度数のカウントを行う形態である。すなわち、認証モジュール117が、認証のみでなく、課金に関する処理も行う形態である。

【0080】

図13に、第2の実施の形態における画面遷移を示す。同図に示すように、第2の実施の形態では、コピーアプリ使用中（状態3）に、コピー枚数が許容枚数をオーバーした場合に、認証モジュール117が警告メッセージを表示する（状態4）。この場合、残度数の更新を行えばコピー画面に戻るが、更新されなければ印刷中止となり認証モジュール画面に戻る。

【0081】

図14の構成図及び図15に示すシーケンスチャートを用いて、第2の実施の形態における複合機100の処理の流れを説明する。なお、図14に示す構成は、複合機100に認証・課金サーバ150がネットワークを介して接続される構成である。

【0082】

認証モジュール画面にてユーザーコード等を入力した後、認証・課金サーバ150が、登録されたユーザーコードと入力されたユーザーコードとを比較することによりユーザー認証を行う。そして、認証が成功した場合に、認証されたユーザーのコピー利用可能枚数（残度数という）が複合機100に送られる（ステップS101）。

【0083】

認証モジュール117はNC S128を介してその残度数を受信し、それを不揮発性RAM、HDD等の記憶装置に保存する（ステップS102）。なお、この残度数は、ユーザー毎に課金する場合にはユーザー単位であり、記憶装置には、ユーザー毎の残度数を記録する。また、例えば部門毎に課金する場合は部門単位に残度数を記録する。

【0084】

認証が成功したことにより、第1の実施の形態で説明したようにオペレーションパネルにアプリ選択指示が表示され、そこでコピーアプリを選択することによりコピーアプリ112に画面制御権限が移行し、コピー画面が表示される。

【0085】

コピーアプリ112は、認証モジュール117に残度数が0より大きいかな否かを問い合わせ、認証モジュール117は、0より大きい場合に印刷OKを返す（ステップS103）。なお、問い合わせはSC S122を介して行うこともできる。また、コピーアプリ112は、残度数の値を記憶装置をチェックすることにより確認してもよい。

【0086】

ユーザーによりコピーが開始されると、コピーアプリ112は、印刷ジョブをEC S124に通知する（ステップS104）。ジョブに応じたEC S124からの命令を受けたコピーエンジン側からは、1枚印刷するたびに、EC S124に対して、印刷完了のイベ

ント通知をし（ステップS105）、そのイベントはSCS122経由で認証モジュール117に通知される（ステップS106）。

【0087】

認証モジュール117は、残度数から印刷枚数を減算して残度数を更新する（ステップS107）。そして、認証モジュール117は、ページ単位又は定期的にNC S128経由で認証・課金サーバ150に残度数を通知する（ステップS108）。

【0088】

残度数が0になると、認証モジュール117からコピーアプリ112に対して印刷中止の通知をする（ステップS109）。なお、この通知はSCS122経由で行うこともできる。その後、コピーアプリはコピージョブをキャンセルして、EC S124に対して印刷中止を通知する（ステップS110）。そして、認証モジュール117は、残度数がない旨の警告表示をオペレーションパネルに対して行う。

【0089】

認証・課金サーバ150側で残度数更新がなされると、新たな残度数が認証モジュール117に通知され（ステップS111）、認証モジュール117からコピーアプリ112に対して残度数更新の通知がされ（ステップS112）、コピーアプリ112は、EC S124に対してコピー再開要求をする（ステップS113）。そして、コピーが再開される。

【0090】

なお、利用中に残度数が0になった場合に、コピー動作を停止する処理をSCS122が行うことも可能である。この場合、例えば、SCS122が「キーカードを通してください」等のポップアップウインドウを表示することで、正しいキーカードを通さない限り、アプリケーションの利用を制限することができる。

【0091】

また、上記の例では認証モジュール117が印刷完了通知を収集することにより、残度数管理を行っているが、これ以外にも、所望のアプリケーションを使用するときに発生する一連の操作や印刷、読みとり、FAX送信などに関する情報をユーザーのIDに関連付けて収集するように構成することが可能である。これにより、誰がいつ何をどの位使用したかのログ情報を管理することが可能となり、そのログ情報に応じて、課金することも可能である。

【0092】

上記のように、第2の実施の形態によれば、認証モジュール117が、印刷完了通知等のログ情報を収集する。ここで、認証モジュール117は、SCS122等のコントロールサービスと異なり、後から追加可能なモジュールであるため、ログ情報の収集方法を変更することが容易であり、市場の要求に応じた課金や利用状況の把握を行うことが可能となる。例えば、紙サイズ、各種印刷条件（両面印刷、集約印刷、ステープル有無等）、印刷枚数、ジャム発生回数等の情報をユーザー毎あるいは部門毎に収集することにより、複合機100の利用状況を把握できる。また、誰がどんな文書を何の目的でコピーしたか、FAXしたか、あるいはスキャンしたかなどの情報を入力させ、収集することにより、より具体的に複合機100の利用状況を管理することが可能となる。これらの情報は、認証画面でユーザーコードやパスワードに加えて、それらの情報も入力しないと利用が許可されないように画面を設計することで、容易に収集することができる。

【0093】

[認証モジュールの構成]

図16に、第1、第2の実施の形態において説明した認証モジュール117の構成の一例を示す。図16に示すように、認証モジュール117は、認証制御部301、認証データ管理部302、利用制限管理部303、及び利用状況管理部304を有している。また、認証制御部301は、操作画面解放判定部3011とキー／イベント／タイマー監視部3012を含んでいる。

【0094】

認証制御部 301 は、電源 ON 後の立ち上がり、システムリセット、又は印刷等のジョブ終了の後、認証モジュール 117 の認証画面を表示する機能を有している。また、認証制御部 301 は、認証画面から入力されたデータ（例えばユーザーコード）が、認証条件を満たすか否かの判定を行う。例えば、入力されたユーザーコードと予め登録されたユーザーコードとを比較し、両者が一致すれば認証成功と判定する。認証が成功しない限り、アプリケーションの使用は許可されない。操作画面解放判定部 3011 は、認証結果に応じて、認証画面を解除して、画面を他のアプリケーションのために解放してよいかどうかを判定する機能を有し、キー／イベント／タイマー監視部 3012 は、入力されるキー、イベント、及び、タイマーのタイムアウトを監視する機能を有する。

【0095】

認証モジュール 117 の中のこの認証制御部 301 の部分を、IC カード、SD カード等の記憶媒体から、もしくはネットワークからのダウンロードにより、複合機 100 に後から追加可能である。

【0096】

認証データ管理部 302 は、ユーザーコード、パスワード等の認証データの管理、及び、体系に沿った情報の管理を行なう。認証データ管理部 302 は、認証制御部 301 からの問い合わせに対し、必要なデータを取得し、認証制御部 301 に返す。また、認証データ管理部 302 が、入力されたデータが認証条件を満たすか否かの判定を行い、その判定結果を認証制御部 301 に返すようにしてもよい。更に、認証データ管理部 302 は認証データの更新／編集機能を有している。

【0097】

利用制限管理部 303 は、認証とは別に、各ユーザー、グループ（組織）単位で、アプリケーション毎に利用制限を行なう機能を有している。例えば、ある部署にのみ特定のアプリケーションの使用を許可することを設定した場合、認証制御部 301 が表示する利用制限画面を介して入力された部署名をその設定内容と比較することにより、特定のアプリケーションの使用可否を決定する。更に、アプリケーション毎の利用制限に加え、各ユーザー、グループ（組織）単位で、特定のアプリケーションの使用量（例えばコピー枚数）の上限を設定する機能を有し、上限に到達すると、その旨を認証制御部 301 に通知する機能を有している。

【0098】

利用状況管理部 304 は、認証されたユーザー、グループ毎に、アプリケーションの利用状況を管理する機能を有している。例えば、コピーであれば枚数を管理し、ネットワークを利用するアプリケーションであれば、データの送信先等のログを管理する。

【0099】

なお、上記各管理部が管理するデータは、複合機 100 のハードディスク等の格納されていてもよいし、ネットワーク接続された外部のサーバに格納されていてもよい。また、上記の各管理部を複合機 100 内に備えることに代えて、ネットワーク接続された外部のサーバに備えてもよい。

【0100】

[認証モジュールの他の構成例]

上記のとおり、本発明の認証モジュール 117 は、システム側に従来から設けられている認証機能（例えば SCS 122 の認証機能）に比べて、追加、変更を容易に行うことができる。すなわち、ユーザーの要望等に応じて変更した認証モジュール 117 を適宜複合機にインストールすることができる。

【0101】

また、認証モジュール 117 を Java（登録商標）プログラムを用いて実装することにより、適宜外部のサーバから Java（登録商標）プログラムを必要に応じてダウンロードしてすぐに実行することが可能となり、更に認証モジュール 117 の追加、変更が容易になる。

【0102】

J a v a (登録商標) プログラムを用いた場合の認証モジュール117 (J a v a (登録商標) プログラム) を含むJ a v a (登録商標) 実行環境118の構成例を図17に示す。このJ a v a (登録商標) 実行環境118は、図3に示す複合機100の構成におけるアプリケーション層に搭載される。

【0103】

図17に示すように、このJ a v a (登録商標) 実行環境118は、J a v a (登録商標) プログラムである認証モジュール117、クラスライブラリ401、仮想マシン402、及びプログラムローダー403を有している。また、図17には、J a v a (登録商標) プログラムを提供するWebサーバ400を示している。複合機100とWebサーバ400はネットワークにより接続されている。

【0104】

クラスライブラリ401は、J a v a (登録商標) プログラムを実行するために必要なクラスライブラリと共に、複合機100を操作するためのサービスを提供するクラスライブラリを含む。仮想マシン402は、J a v a (登録商標) プログラムを解釈し、実行するためのものである。また、プログラムローダー403は、Webサーバ400からのプログラムダウンロード、J a v a (登録商標) プログラムの実行管理等を行うものである。このような環境において、開発されたJ a v a (登録商標) プログラムをWebサーバ400にアップロードしておく。そして、プログラムローダー403がWebサーバ400にアクセスし、ユーザ所望のJ a v a (登録商標) プログラムをダウンロードし、実行する。

【0105】

(第3の実施の形態)

次に、本発明の第3の実施の形態について説明する。第3の実施の形態では、システム側が固定的に有している認証機能 (S C S 1 2 2 等であり、以下、これをシステム側認証制御部と称する) と、本発明に係る認証モジュール117とを切り替えて用いる場合の例について説明する。以下、システム側認証制御部を使用して認証を行うモードを標準認証モードと呼び、本発明に係る認証モジュール117を使用して認証を行うモードを追加認証モードと呼ぶ。

【0106】

[システム側認証制御部による認証画面を利用する例]

まず、システム側認証制御部により表示される認証画面を利用して、システム側認証制御部もしくは認証モジュール117による認証を行う場合について説明する。

【0107】

本実施の形態では、システムの初期設定画面等により、アプリケーション毎に標準認証モードによる認証を行うか、もしくは追加認証モードによる認証を行うかの設定をする。図18に、設定内容の例を示す。図18に示す例では、コピーアプリ、追加アプリ2に標準認証モードが設定され、スキャナアプリ、追加アプリ1には追加認証モードが設定されている。なお、F A X アプリに対しては認証による利用制限をしない設定となっている。

【0108】

また、この例の場合、複合機100の構成を模式的に表した図19に示すように、追加認証モードのときに、システム側認証制御部501により表示される認証画面から入力されたデータが認証モジュール117に渡され、認証モジュール117による認証結果がシステム側認証制御部501に通知される。なお、システム側認証制御部501による認証画面は、図20に示すようなユーザーにユーザコードとパスワードを入力させるための画面である。この認証画面を認証画面Aと呼ぶ。

【0109】

次に、図21に示すフローチャートを参照して、処理の流れを説明する。

【0110】

複合機の電源ONの後 (ステップS201)、オペレーションパネルにシステム側認証制御部501が認証画面Aを表示する (ステップS202)。ユーザーは、オペレーショ

ンパネルのアプリ切り替えキーを押下げることにより、利用したいアプリケーションを選択する（ステップS203）。また、ユーザーは、システム側認証制御部501による認証画面からユーザーコードとパスワードを入力する（ステップS204）。システム側認証制御部501はこれらのキー情報を取得する。

【0111】

システム側認証制御部501は、選択されたアプリケーションに対する認証モードを、図18に示す設定内容から確認し（ステップS205）、標準認証モードであれば、複合機100のシステム側で管理されている予め登録されたデータと、入力されたデータとを比較することによりシステム側認証制御部501が認証を行う（ステップS206）。認証成功であれば、認証画面Aに代えて、選択されたアプリケーションの画面が表示される（ステップS207）。

【0112】

認証モードの設定内容が追加認証モードである場合は、システム側認証制御部501は、認証モジュール117にユーザーコードとパスワードを渡す（ステップS208）。

【0113】

認証モジュール117では、システム側認証制御部501から渡されたユーザーコードとパスワードを基に、認証モジュール117が管理している認証データや利用制限データを参照して認証を行い（ステップS209）、当該アプリケーションが当該ユーザーにより利用可能であれば、システム側認証制御部501に対して利用可能通知を返す（ステップS210）。なお、認証モジュール117が、外部のサーバへユーザーコードとパスワードを送信することにより問い合わせを行う場合には、当該サーバからの結果を待って、システム側認証制御部501への通知を行う。認証成功の通知を受けたシステム側認証制御部501は、最初に表示していた認証画面Aに代えて、アプリケーションの画面の表示を許可し、アプリケーションの画面が表示される（ステップS211）。

【0114】

[システム側認証制御部による認証画面と認証モジュールによる認証画面を利用する例]
次に、システム側認証制御部501による認証画面Aと認証モジュール117による認証画面の両方を利用する場合について説明する。この例における認証モードの設定内容は上記と同様に図18に示す通りである。

【0115】

この例の場合、図22に示す通り、設定内容に応じて、追加認証モードに設定されているアプリケーションに対しては認証モジュール117により表示される認証画面を用いて認証モジュール117による認証が行われ、標準認証モードに設定されているアプリケーションに対してはシステム側認証制御部501により表示される認証画面Aを用いてシステム側認証制御部501により認証が行われる。また、システム側認証制御部501と認証モジュール117間では、画面解放等に関する情報がやり取りされる。認証モジュール117により表示される認証画面の例を図23に示す。この画面を認証画面Bと呼ぶ。

【0116】

次に、図24に示すフローチャートを参照して、処理の流れを説明する。なお、以下の処理は、予め認証モジュールが優先アプリとして設定されている場合の例である。

【0117】

まず、複合機100の電源ONの後（ステップS301）、オペレーションパネルに認証モジュール117が認証画面Bを表示する（ステップS302）。ユーザーが、オペレーションパネルのアプリ切り替えキーを押下げることにより、利用したいアプリケーションを選択すると（ステップS303）、認証モジュール117は、認証モードの設定内容を確認し、選択されたアプリケーションが追加認証モードに対応するのか、もしくは標準認証モードに対応するのかを判断する（ステップS304）。

【0118】

選択されたアプリケーションが標準認証モードに対応する場合、当該アプリケーションは認証モジュール117の管理対象外なので、オペレーションパネルの画面表示部の制御

権限をシステム側認証制御部 501 に渡す (ステップ S305)。これにより、システム側認証制御部 501 は認証画面 A を表示する (ステップ S306)。

【0119】

そして、システム側認証制御部 501 は、この画面から入力されるユーザーコードとパスワードを用いて認証を行い (ステップ S307)、認証が成功であれば、選択されたアプリケーションの画面が表示され (ステップ S308)、ユーザーによるアプリケーションの利用が可能になる。

【0120】

一方、選択されたアプリケーションが追加認証モードに対応する場合、当該アプリケーションは認証モジュール 117 の管理対象なので、既に表示されている認証モジュール 117 の認証画面 B から入力されたデータに基づき、認証モジュール 117 が認証を行う (ステップ S309)。認証が成功であれば、選択されたアプリケーションの画面が表示され (ステップ S311)、ユーザーによるアプリケーションの利用が可能になる。

【0121】

各アプリケーションの使用に際しては、第 1 の実施の形態で説明したように、印刷などの Job 完了、システムオートクリア等をトリガーとして、認証モジュール 117 の認証画面に戻る。

【0122】

また、システム側認証制御部 501 による認証画面 A、もしくはアプリケーションの画面が表示された状態で、別のアプリケーションへの切り替えが行われた場合、そのアプリケーションが認証モジュール 117 の管理対象であれば、切り替えが行なわれたときに認証モジュール 117 の認証画面 B に画面が遷移する。

【0123】

(第 4 の実施の形態)

次に、本発明の第 4 の実施の形態について説明する。

【0124】

これまでに説明した実施の形態では、ユーザーからのデータ入力を複合機 100 のオペレーションパネルから行っていたが、PDA (携帯情報端末: personal digital assistant) や、データ通信機能を持つ携帯電話から、認証のためのデータを入力することが可能である。本実施の形態では、PDA や携帯電話からデータを入力する場合について説明する。

【0125】

図 25 に、複合機 100 と PDA 601、携帯電話 602 等が通信を行う場合の構成を示す。図 25 に示すように、複合機 100 はネットワーク 603 (LAN もしくはインターネット等の WAN) に接続される。接続は、有線でもよいし、無線 LAN カード 604 を介して無線で行ってもよい。また、複合機 100 に、アドホックネットワークを用いて PDA 601 と直接接続する機能を備えてもよい。更に、複合機 100 に、携帯電話 602 と内線により通信できる機能を備えてもよい。

【0126】

また、複合機 100 は、データ通信プロトコル処理機能 605、Web サーバ機能 606、認証画面データを生成する画面データ生成機能 607 を備える。なお、画面データ生成機能 607 は例えば認証モジュール 117 に備えられる。その他の複合機 100 の構成は、これまでの実施の形態で説明したものと同様である。このような構成により、PDA 601 や携帯電話 602 と複合機 100 との間でデータ通信を行うことができる。以下、認証時の動作を説明する。以下の説明においては、PDA 601、携帯電話 602 を総称して携帯端末と呼ぶ。

【0127】

まず、複合機 100 の URL もしくは IP アドレスを指定することにより、携帯端末が複合機 100 にアクセスする。アクセスを受けた複合機 100 は、認証に必要な情報を要求する画面に対応する HTML データもしくは XML データを生成し、それを携帯端末に

返す。

【0128】

画面のデータを受信した携帯端末は図20もしくは図23に示すような画面を携帯端末の画面表示部に表示する。そして、携帯端末のユーザーが、必要な認証データを入力して複合機100に対してそのデータを送信する。

【0129】

なお、携帯端末に認証データを一度登録しておけば次回からの操作が簡単になる。また、携帯電話と複合機100が内線で通信を行う場合、予め複合機100に内線番号を割り振り、複合機100に発呼する際に、認証データを付加して送るようにすれば、更に簡単に認証作業を行なうことができる。

【0130】

認証データを受信した複合機100は、例えば第3の実施の形態で説明した方法により認証を行い、認証が成功であれば複合機100の画面がアプリケーションの画面に切り替わり、当該アプリケーションが使用可能となる。なお、アプリケーションの選択は複合機100側で行ってもよいし、携帯端末から行ってもよい。

【0131】

本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【0132】

【図1】 複合機の外觀例と、オペレーションパネルを示す図である。

【図2】 複合機100と認証・課金サーバ150とがネットワークを介して接続された構成を示す図である。

【図3】 複合機100の構成を示すブロック図である。

【図4】 複合機100の構成を示すブロック図である。

【図5】 複合機100のハードウェア構成図である。

【図6】 複合機100の立ち上げ時の動作を示すフローチャートである。

【図7】 アプリ設定ファイルを説明するための図である。

【図8】 アプリ設定ファイルの内容例を示す図である。

【図9】 SCS122の起動後の複合機100の動作を示すフローチャートである。

【図10】 優先アプリの設定を説明するための図である。

【図11】 第1の実施の形態におけるオペレーションパネル210の画面状態遷移図である。

【図12】 第1の実施の形態における認証モジュールの動作を説明するためのシーケンスチャートである。

【図13】 第2の実施の形態における画面状態遷移図である。

【図14】 第2の実施の形態における複合機100の処理の流れを説明するための構成図である。

【図15】 第2の実施の形態における複合機100の処理の流れを説明するためのシーケンスチャートである。

【図16】 認証モジュール117の構成の一例を示す図である。

【図17】 認証モジュール117（Java（登録商標）プログラム）を含むJava（登録商標）実行環境118の構成例である。

【図18】 認証モードの設定内容を示す図である。

【図19】 第3の実施の形態における認証方法を説明するための図である。

【図20】 システム側認証制御部により表示される認証画面Aである。

【図21】 システム側認証制御部による認証画面を利用する場合のフローチャートである。

【図22】 第3の実施の形態における認証方法を説明するための図である。

【図23】 認証モジュールにより表示される認証画面Bである。

【図 2 4】システム側認証制御部による認証画面と認証モジュールによる認証画面を利用する場合のフローチャートである。

【図 2 5】複合機 1 0 0 と P D A 6 0 1、携帯電話 6 0 2 等が通信を行う場合の構成を示す図である。

【符号の説明】

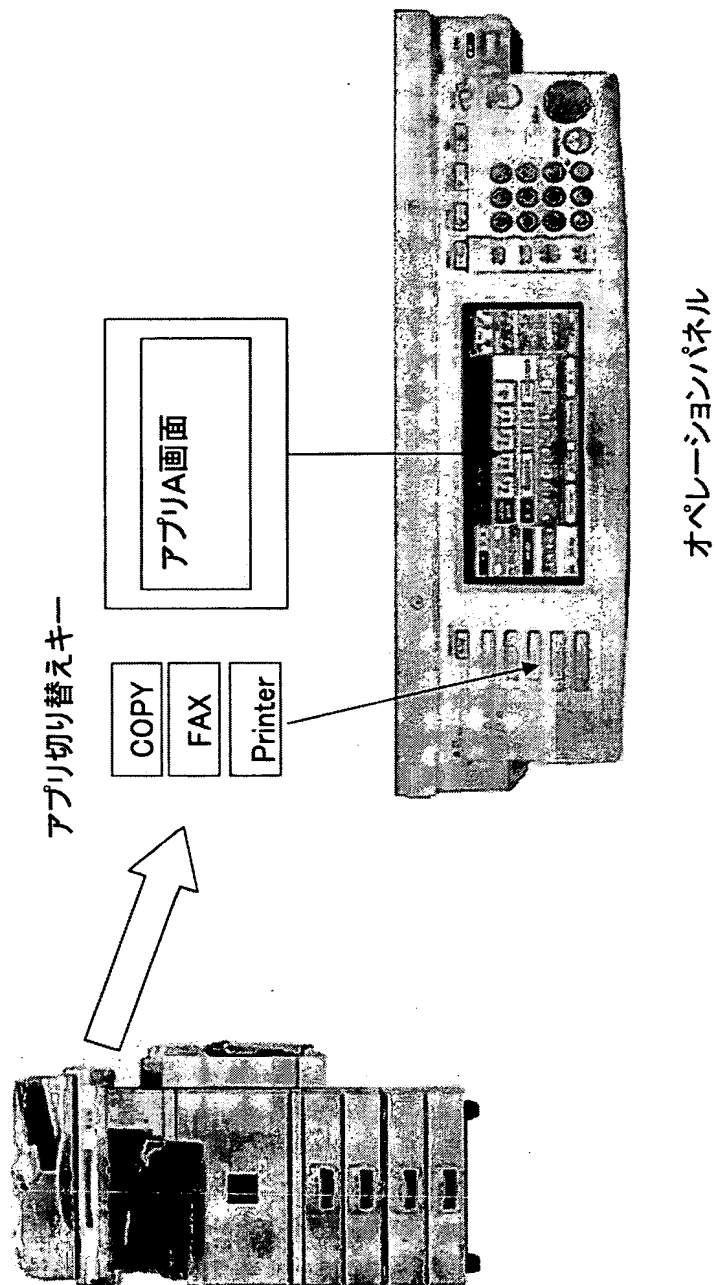
【 0 1 3 3 】

- 1 0 0 複合機
- 1 0 1 白黒ラインプリンタ
- 1 0 2 カラーラインプリンタ
- 1 1 0 ソフトウェア群
- 1 1 1 プリンタアプリ
- 1 1 2 コピーアプリ
- 1 1 3 ファックスアプリ
- 1 1 4 スキャナアプリ
- 1 1 5、1 1 6 追加アプリ
- 1 1 7 認証モジュール
- 1 1 8 J a v a（登録商標）実行環境
- 1 2 0 プラットホーム
- 1 2 1 汎用 O S
- 1 2 2 S C S
- 1 2 3 S R M
- 1 2 4 E C S
- 1 2 5 M C S
- 1 2 6 O C S
- 1 2 7 F C S
- 1 2 8 N C S
- 1 3 0 アプリケーション
- 1 4 0 複合機起動部
- 1 5 0 認証・課金サーバ
- 2 0 0 コントローラボード
- 2 0 1 A S I C
- 2 0 2 C P U
- 2 0 3 R A M
- 2 0 4 R O M
- 2 0 5 H D D
- 2 0 6 フラッシュカードインタフェース部
- 2 0 7 フラッシュカード
- 2 0 9 ネットワークコントロールインターフェース
- 2 1 0 オペレーションパネル
- 2 2 0 F C U
- 2 3 0 U S B
- 2 4 0 I E E E 1 3 9 4
- 2 5 0 ブルートゥース
- 2 6 0 エンジン部
- 3 0 1 認証制御部
- 3 0 2 認証データ管理部
- 3 0 3 利用制限管理部
- 3 0 4 利用状況管理部
- 4 0 0 W e b サーバ
- 4 0 1 クラスライブラリ

- 4 0 2 仮想マシン
- 4 0 3 プログラムローダー
- 5 0 1 システム側認証制御部
- 6 0 1 P D A
- 6 0 2 携帯電話
- 6 0 3 ネットワーク
- 6 0 4 無線 L A N カード
- 6 0 5 データ通信処理機能
- 6 0 6 W e b サーバ機能
- 6 0 7 画面データ生成機能

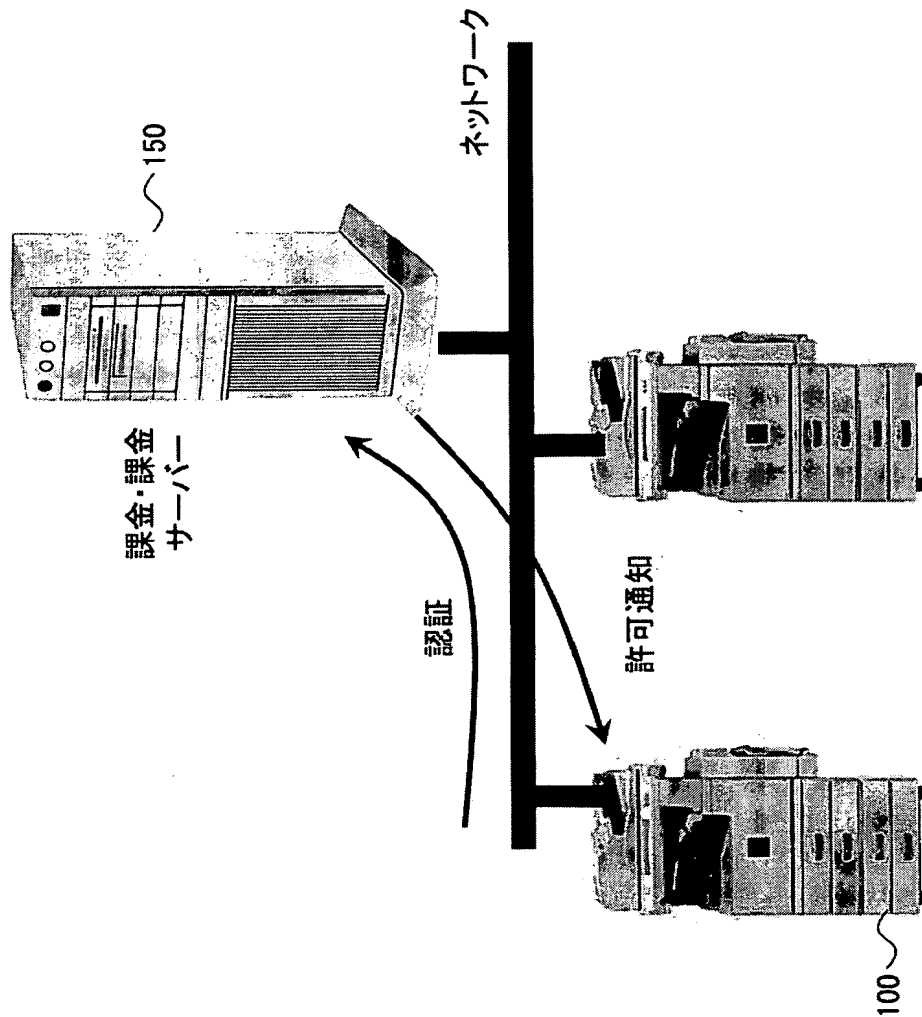
【書類名】 図面
【図 1】

複合機の外觀例と、オペレーションパネルを示す図



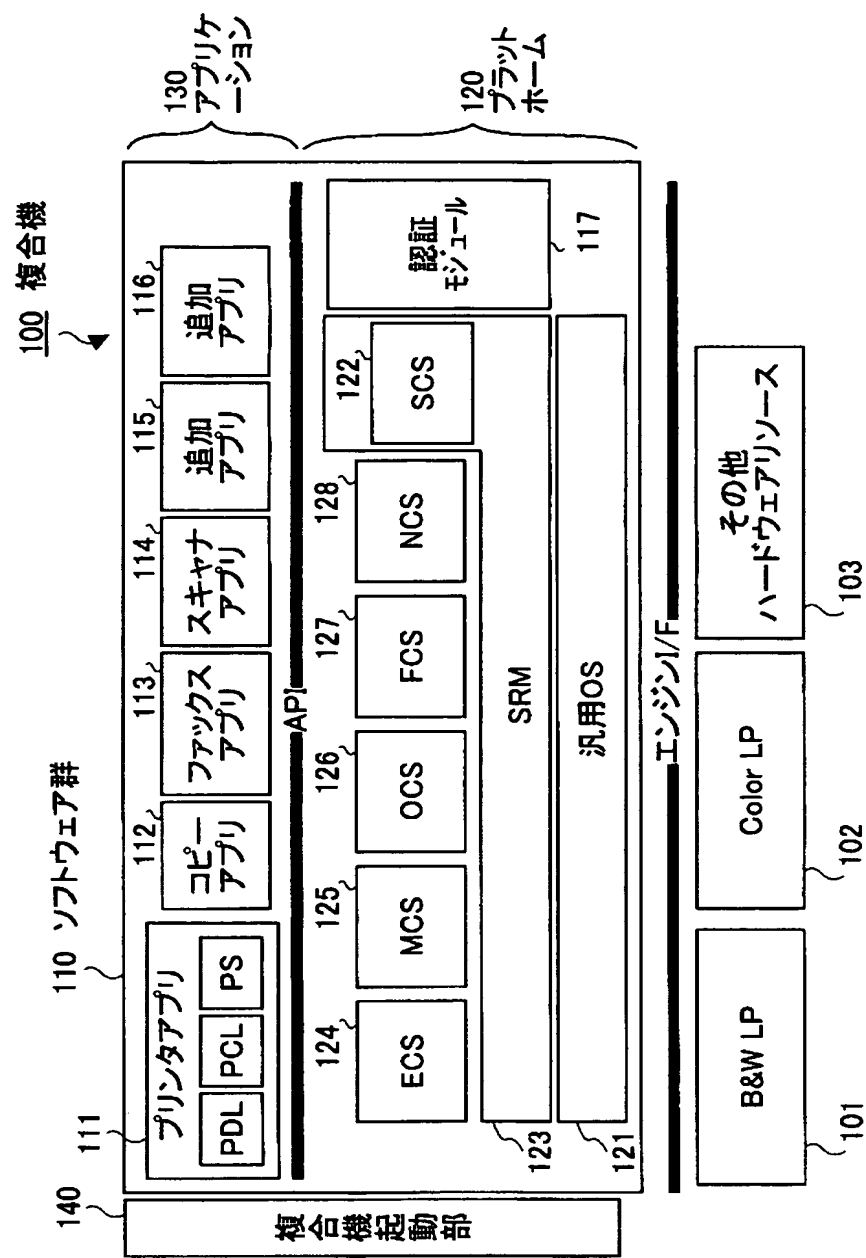
【図 2】

複合機100と認証・課金サーバ150とがネットワークを介して
接続された構成を示す図



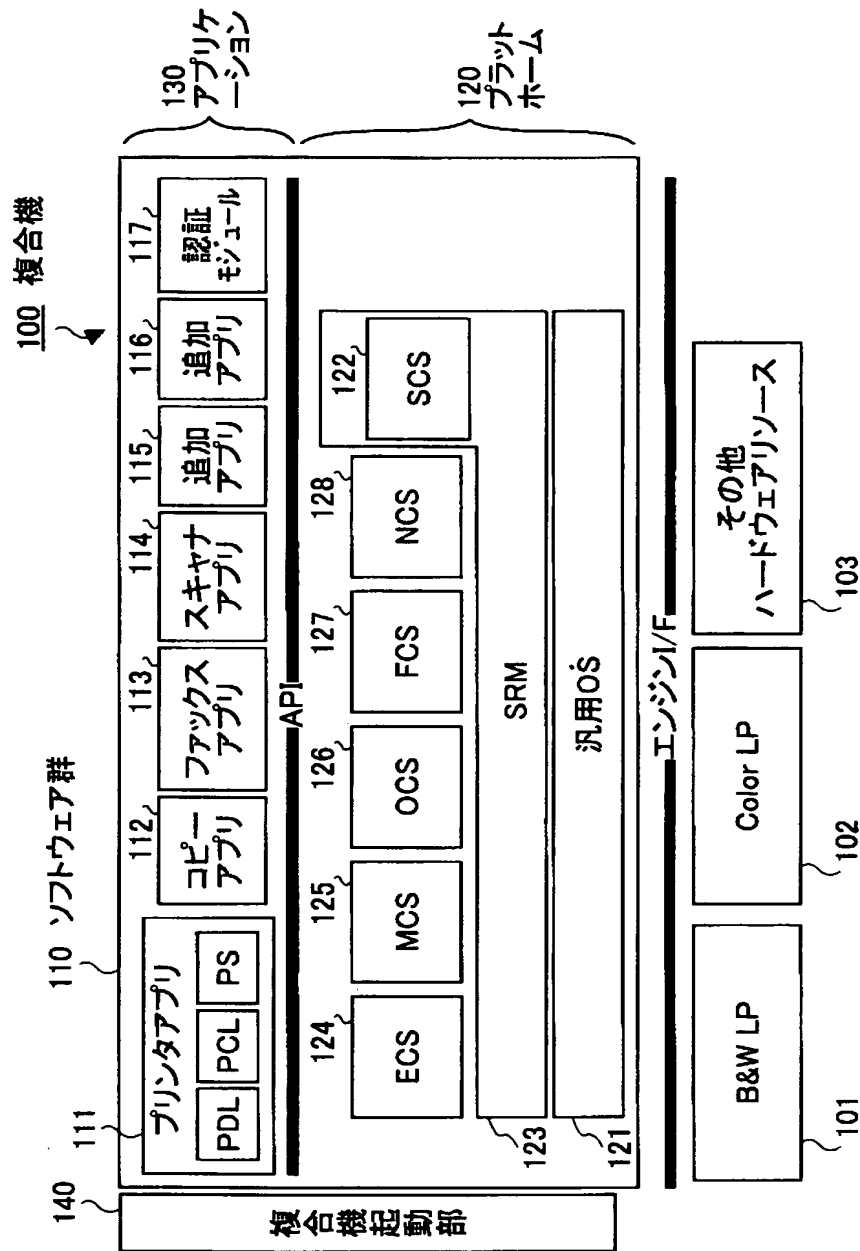
【図 3】

複合機100の構成を示すブロック図



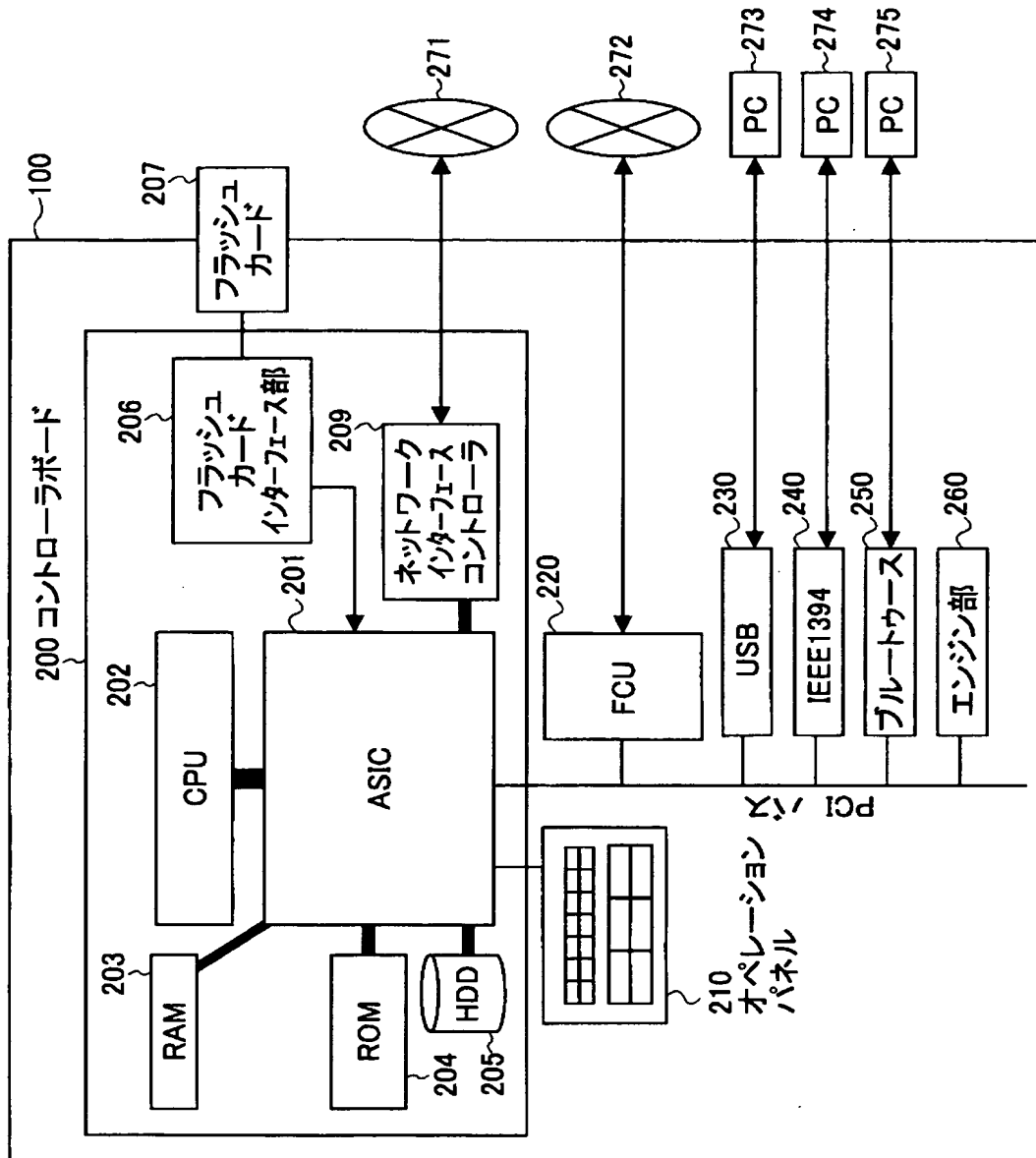
【図 4】

複合機100の構成を示すブロック図



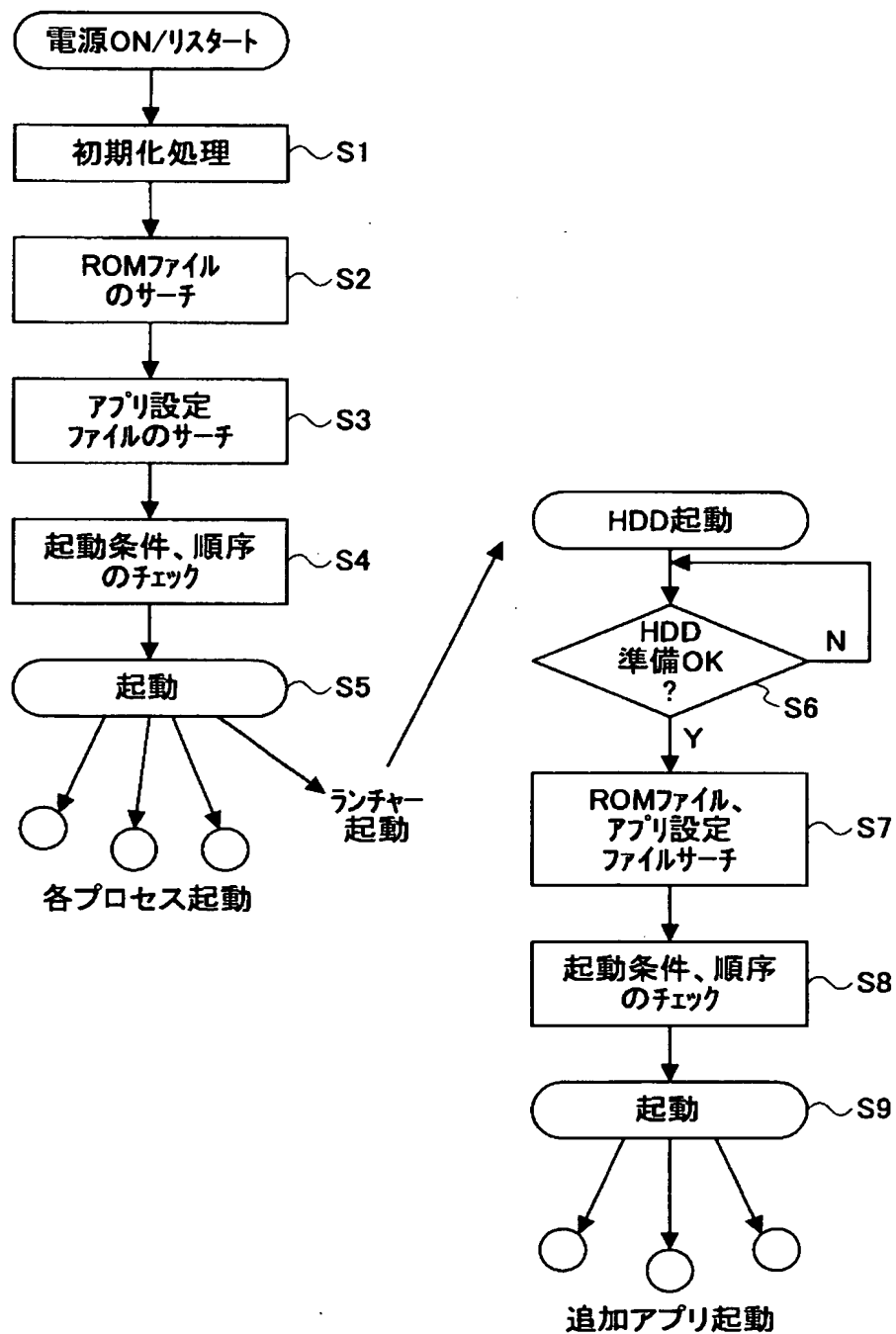
【図 5】

複合機100のハードウェア構成図



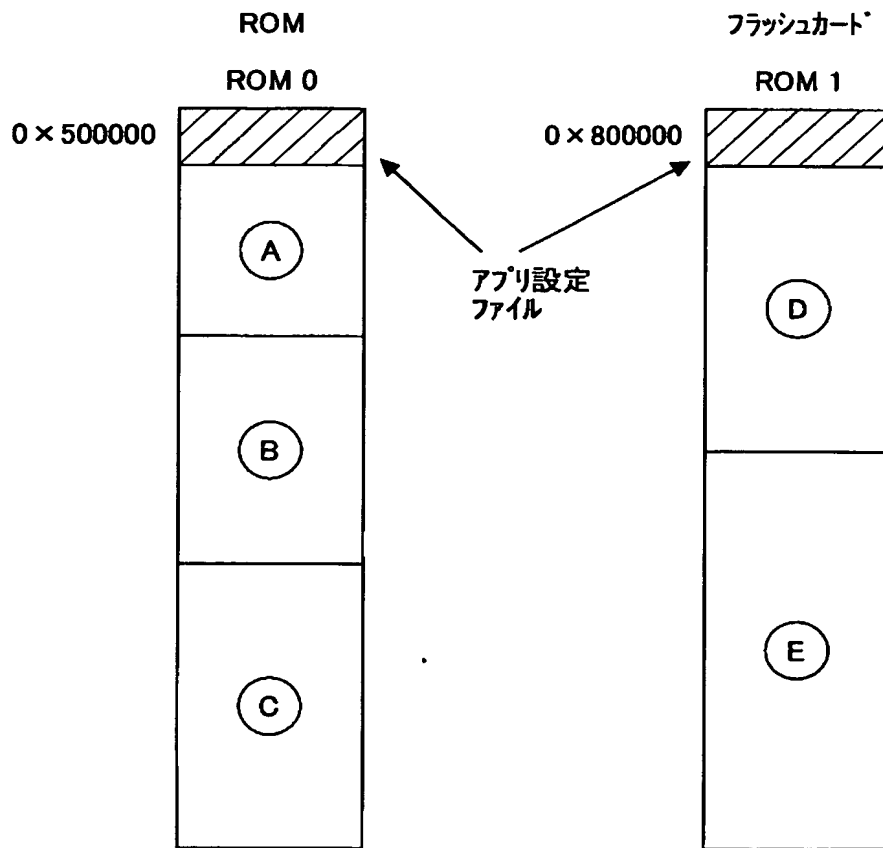
【図 6】

複合機100の立ち上げ時の動作を示すフローチャート



【図 7】

アプリ設定ファイルを説明するための図



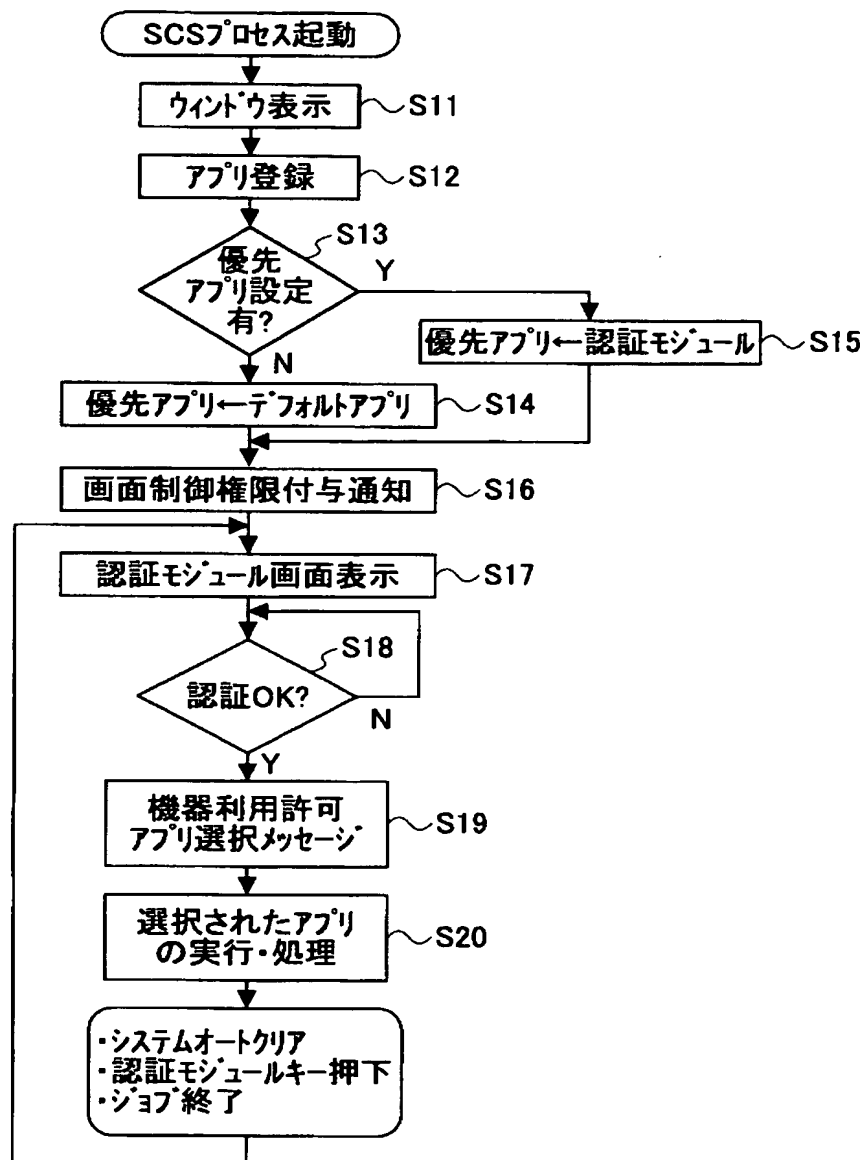
【図 8】

アプリ設定ファイルの内容例を示す図

(a)	mount	romfs	0 × 500000	ROM 0
	mount	romfs	0 × 800000	ROM 1
	exec	-2	/bin/Ⓐ	
	exec	-5	/bin/Ⓑ	
	exec	-3	/bin/Ⓒ	
(b)	exec	-2	/bin/Ⓓ	
	exec	-3	/bin/Ⓔ	

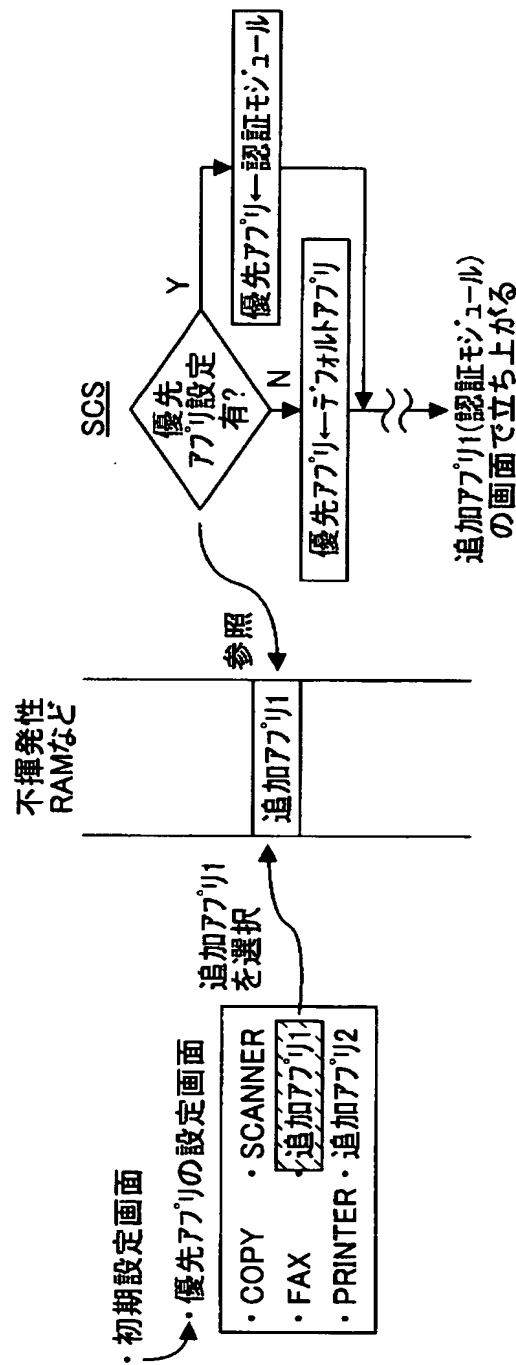
【図 9】

SCS122の起動後の複合機100の動作を示すフローチャート

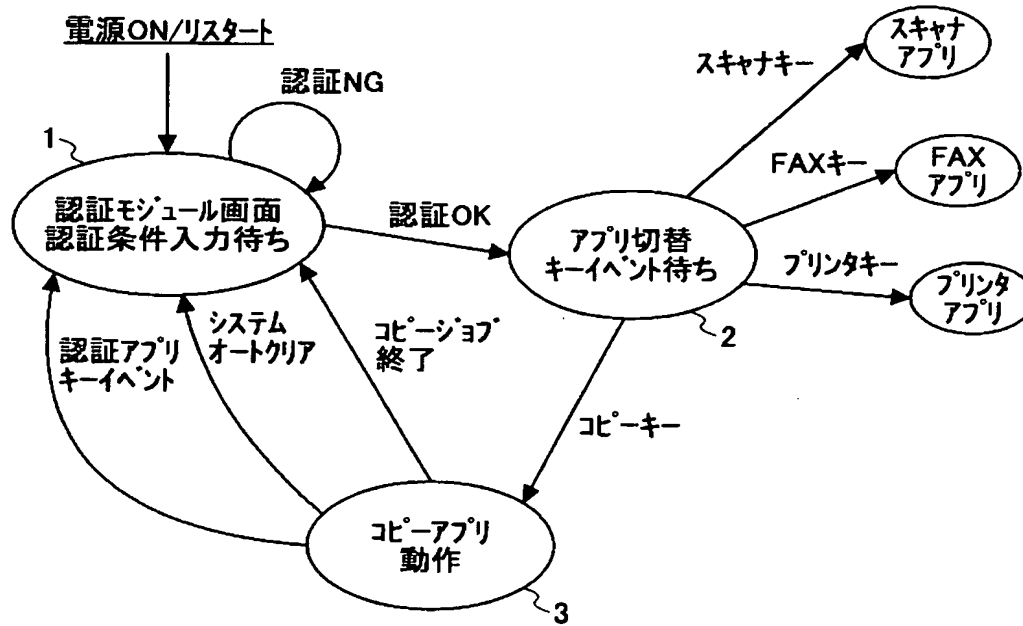


【図 10】

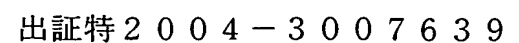
優先アプリの設定を説明するための図



【図 11】

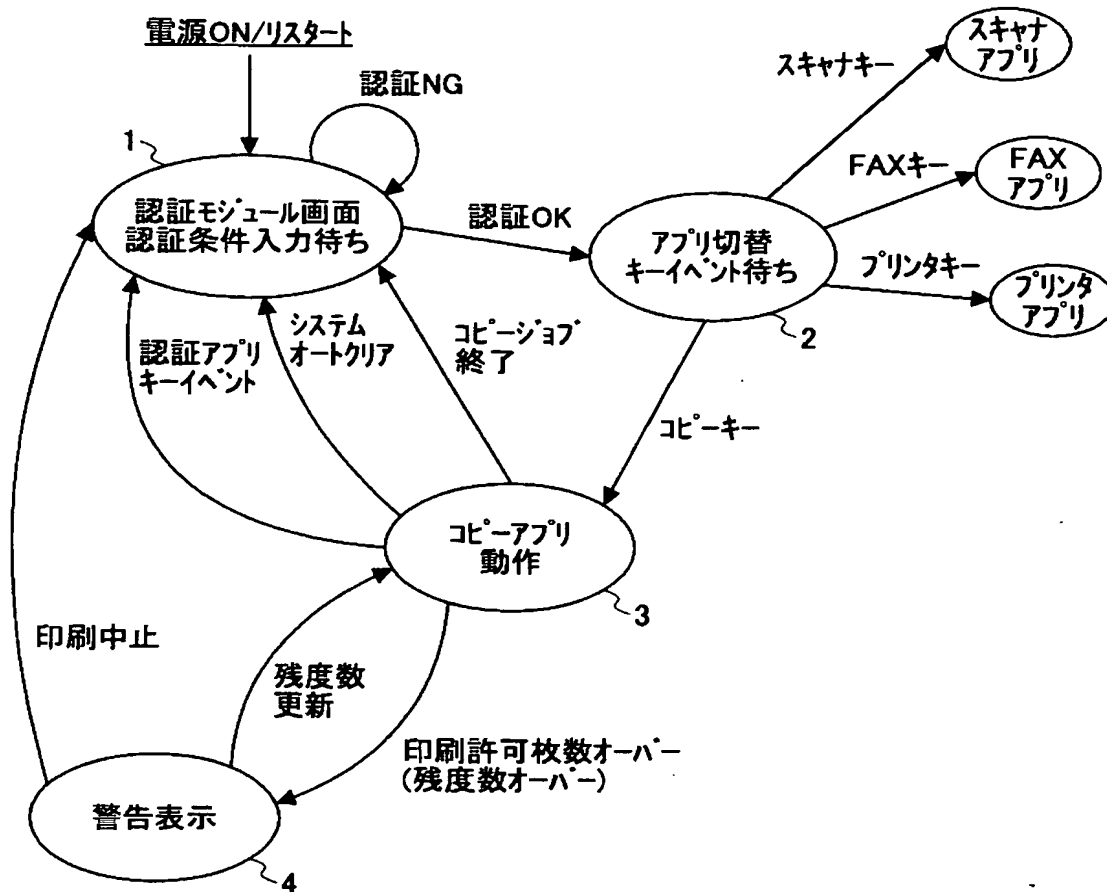
第1の実施の形態におけるオペレーションパネル210の
画面状態遷移図

第1の実施の形態における認証モジュールの動作を説明するためのシーケンスチャート



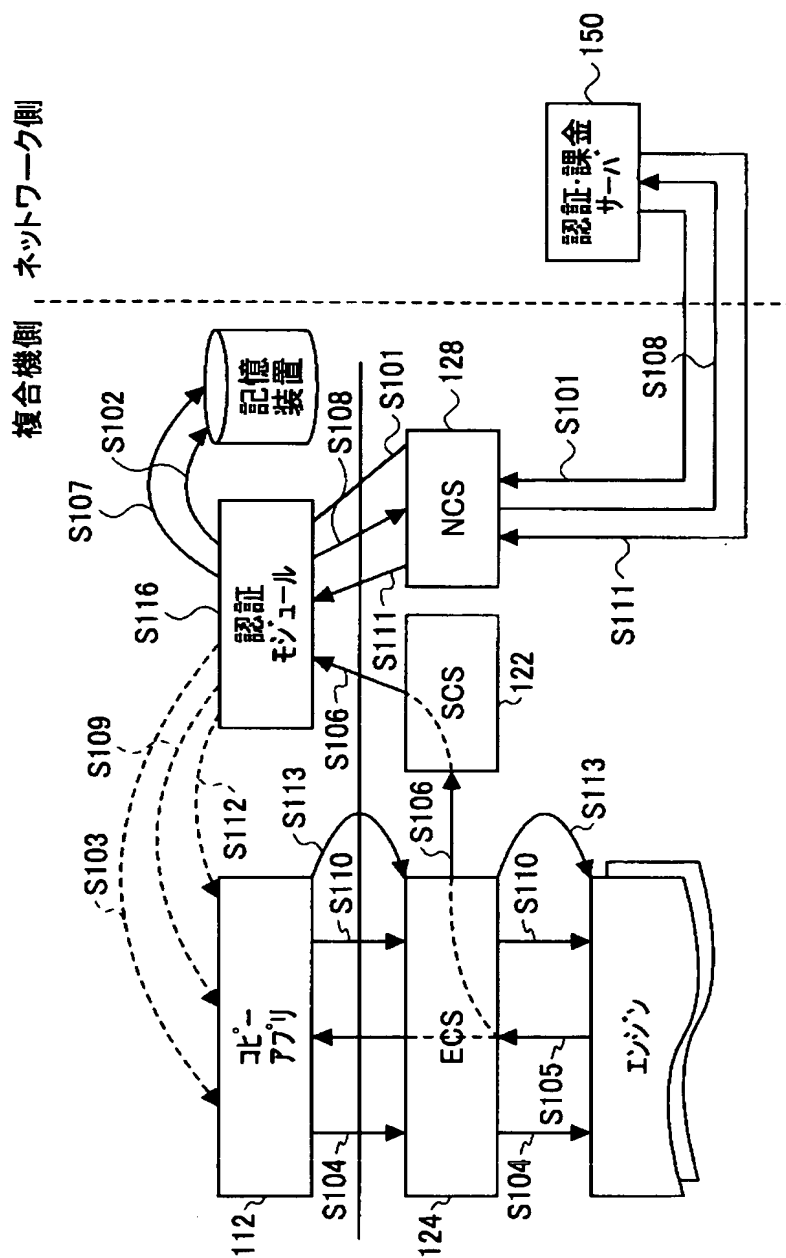
【図 13】

第2の実施の形態における画面状態遷移図



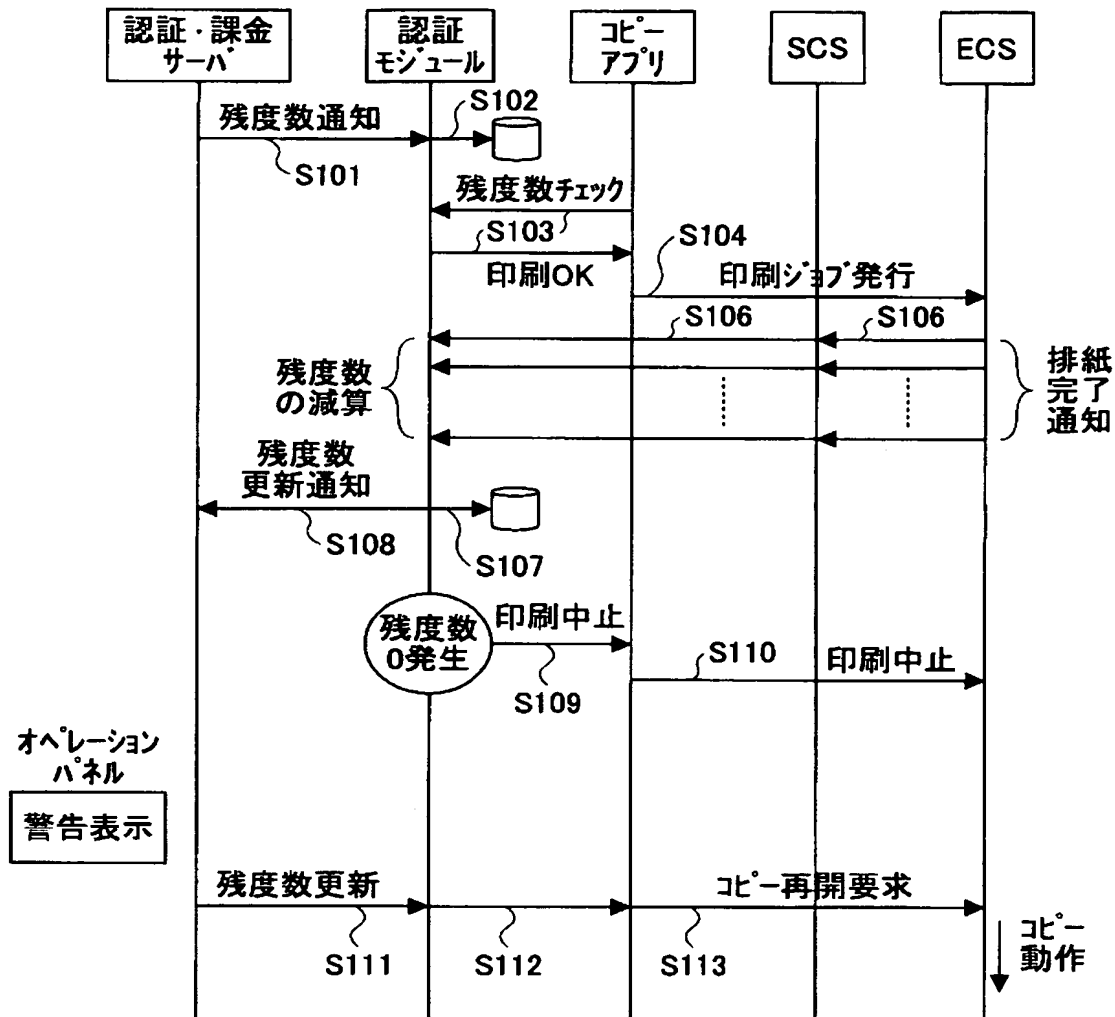
【図 14】

第2の実施の形態における複合機100の 処理の流れを説明するための構成図



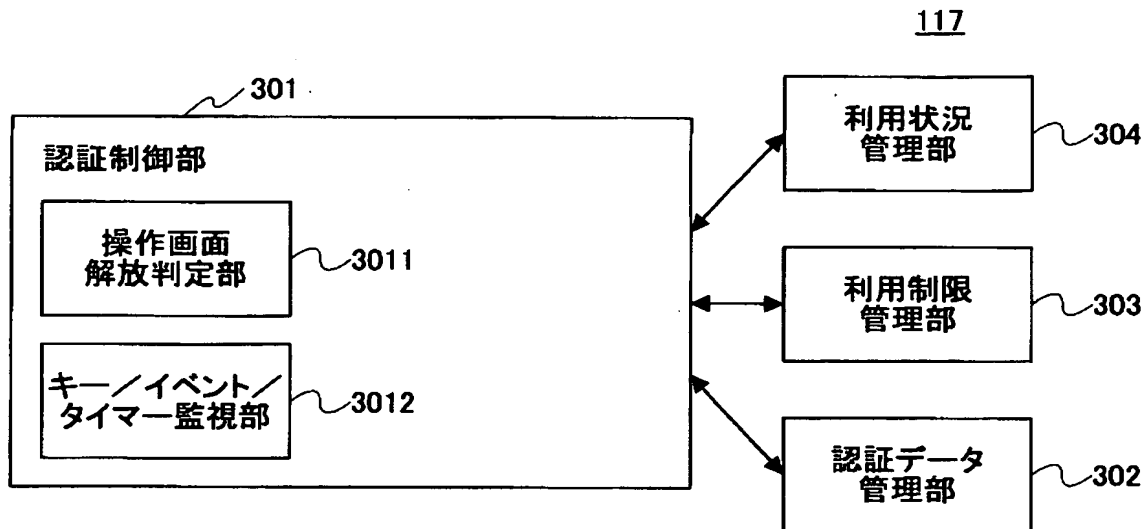
【図 15】

第2の実施の形態における複合機100の処理の
流れを説明するためのシーケンスチャート

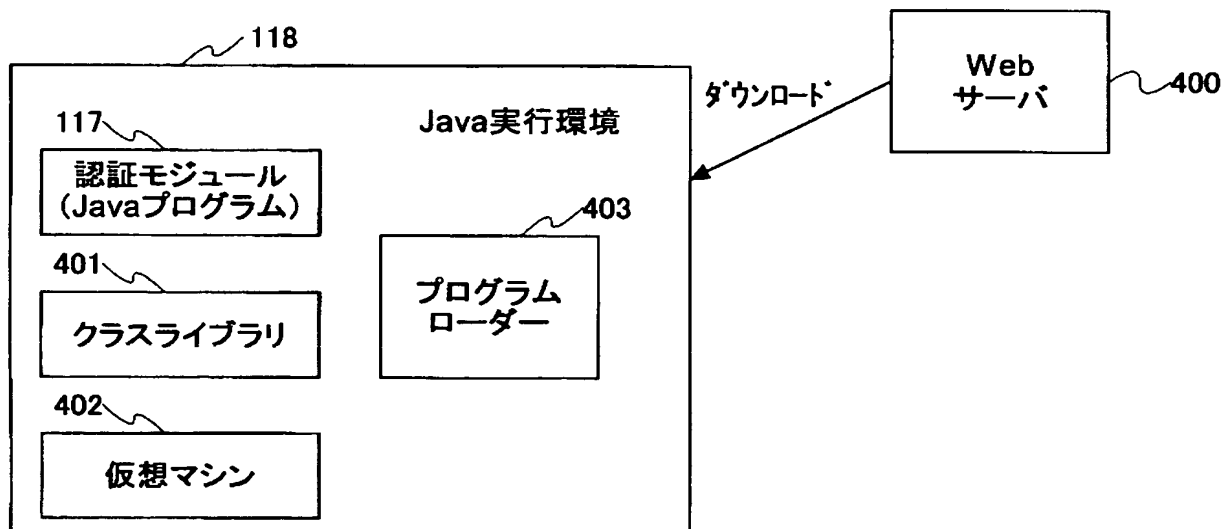


【図 16】

認証モジュール 117 の構成の一例を示す図



【図 17】

認証モジュール 117 (Java プログラム) を含む
Java 実行環境 118 の構成例

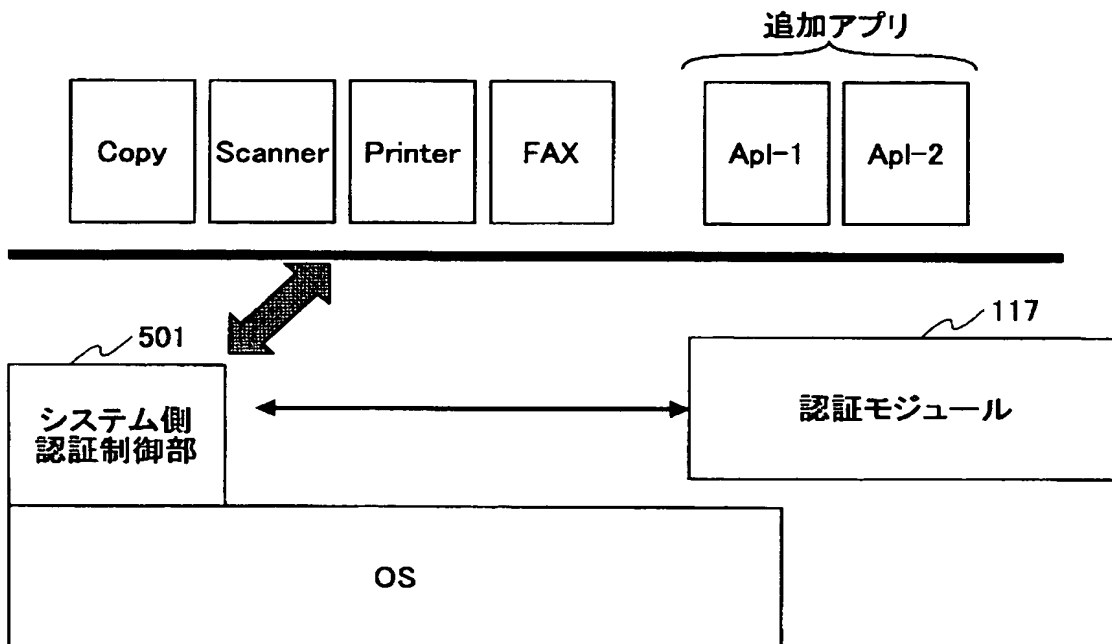
【図 18】

認証モードの設定内容を示す図

■システム設定		
	利用制限 する／しない	認証モード
Copy	する	標準
スキャナ	する	追加
FAX	しない	-
追加アプリ1	する	追加
追加アプリ2	する	標準

【図 19】

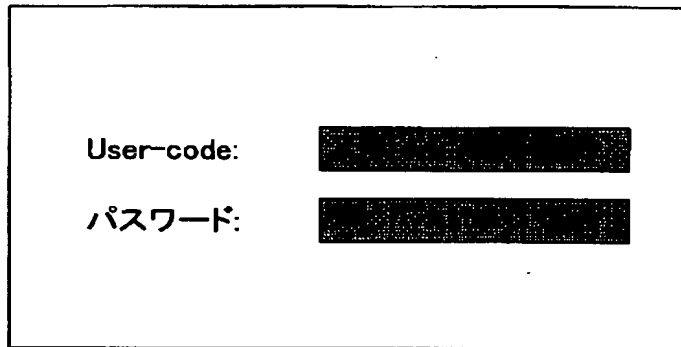
第3の実施の形態における認証方法を説明するための図



【図 2 0】

システム側認証制御部により表示される認証画面 A

認証画面 A

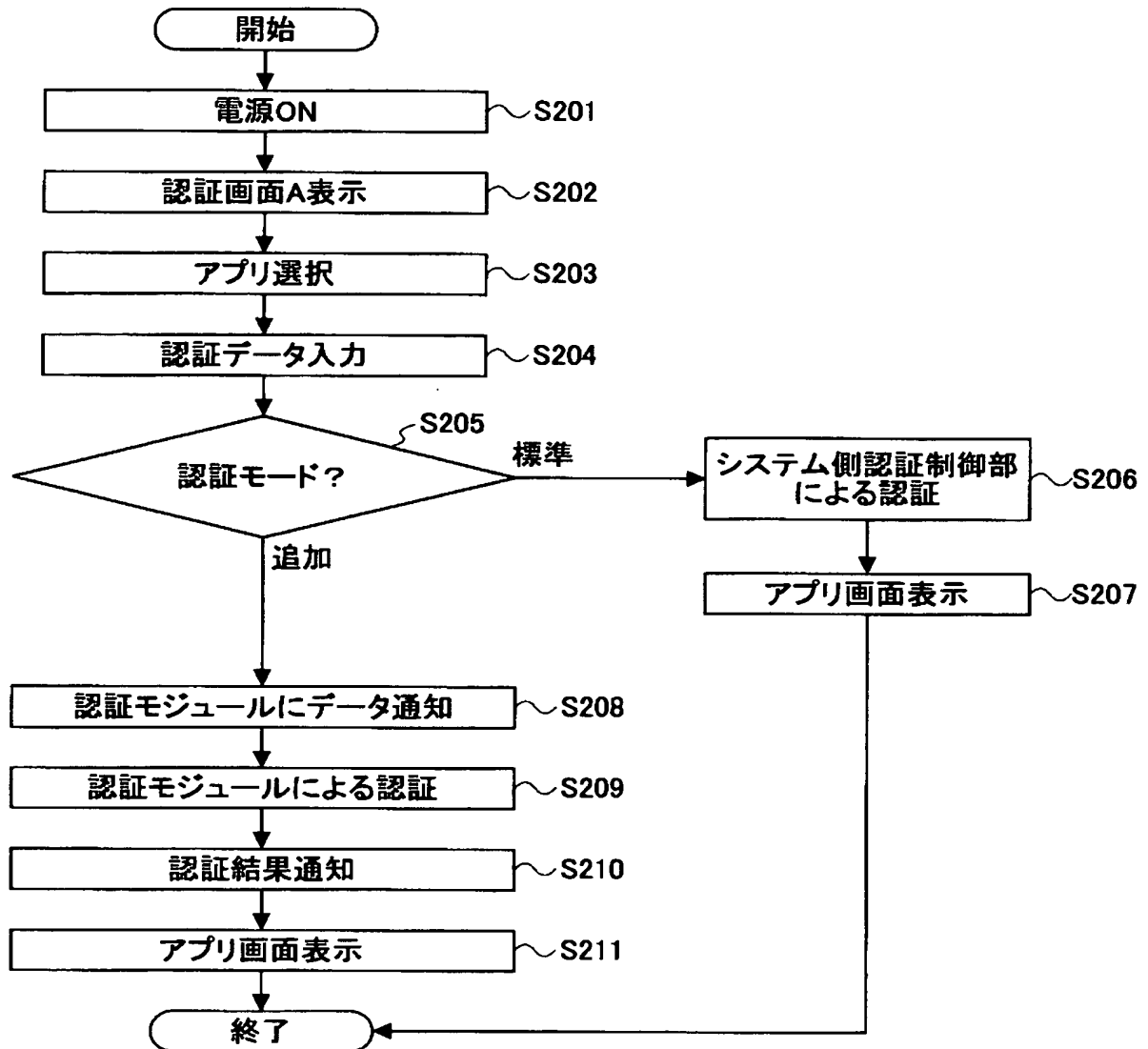


The image shows a rectangular box representing a screen. Inside the box, there are two labels on the left and two corresponding input fields on the right. The top label is 'User-code:' and the bottom label is 'パスワード:'. Both input fields are represented by black rectangular boxes, indicating that the content has been redacted for security.

User-code:	[Redacted]
パスワード:	[Redacted]

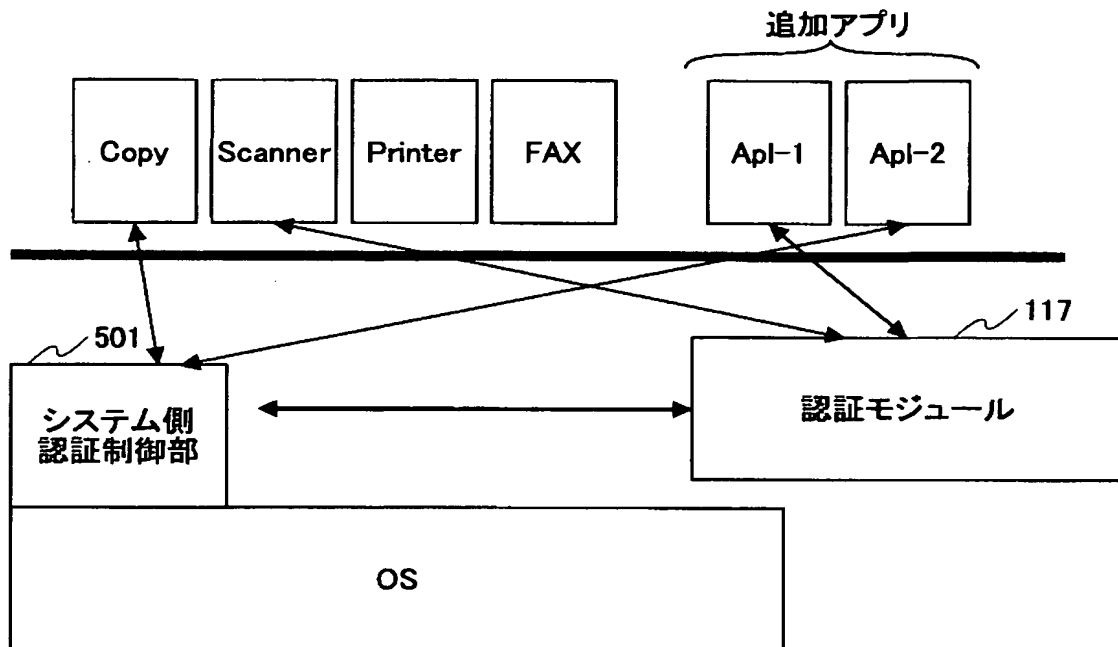
【図 21】

システム側認証制御部による認証画面を利用する場合のフローチャート



【図 22】

第3の実施の形態における認証方法を説明するための図



【図 23】

認証モジュールにより表示される認証画面B

認証画面 B

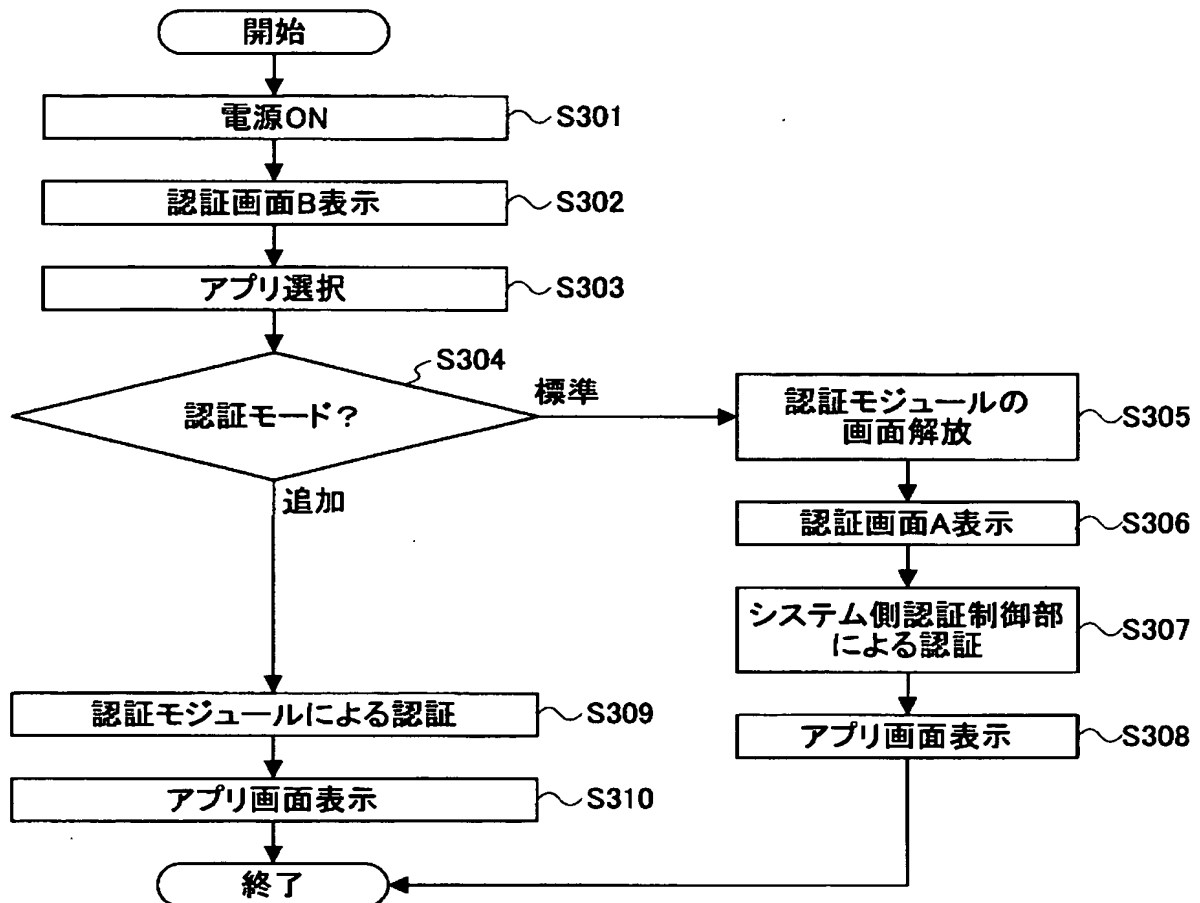
User-code:

パスワード:

部門選択

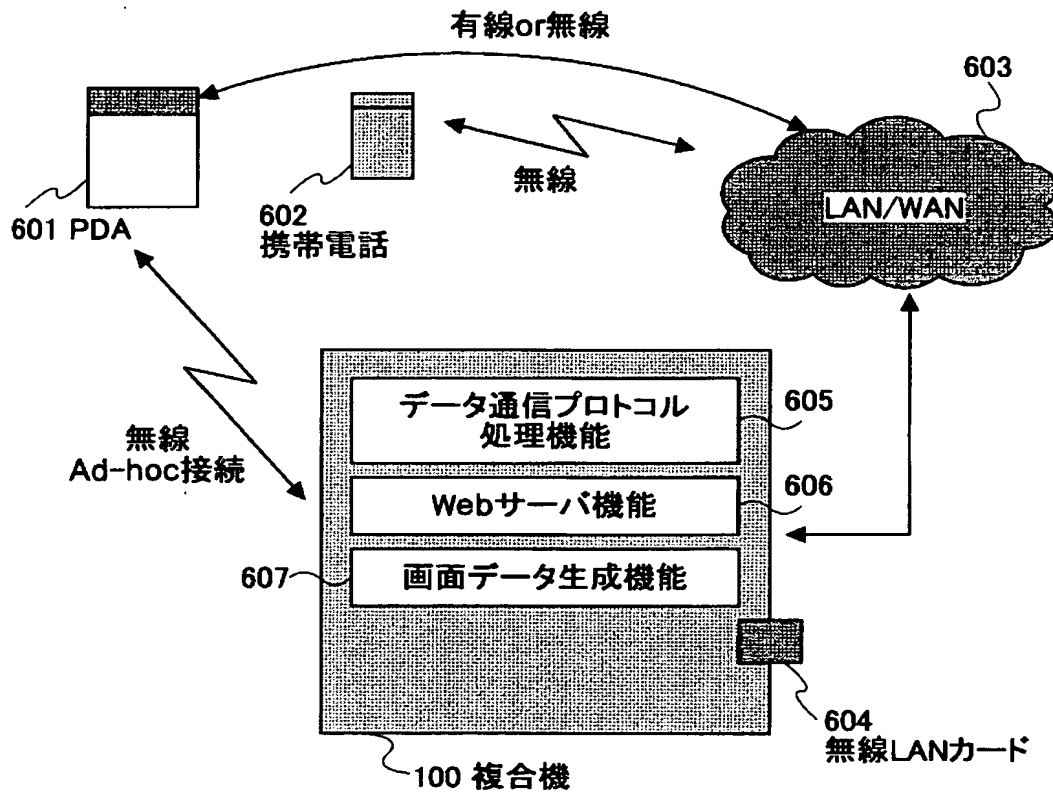
【図 24】

システム側認証制御部による認証画面と認証モジュールによる
認証画面を利用する場合のフローチャート



【図 25】

複合機100とPDA601、携帯電話602等が
通信を行う場合の構成を示す図



【書類名】 要約書**【要約】**

【課題】 種々の目的に応じた認証機能を容易に追加、変更することを可能とする。

【解決手段】 アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置において、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、当該認証モジュールを前記システム側ソフトウェアとは別に備えるように構成した。

【選択図】 図 3

特願 2 0 0 4 - 0 1 2 9 0 4

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 6 7 4 7]

1. 変更年月日	2 0 0 2 年 5 月 1 7 日
[変更理由]	住所変更
住 所	東京都大田区中馬込 1 丁目 3 番 6 号
氏 名	株式会社リコー